

#3

LAW OFFICES
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC

2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213
TELEPHONE (202) 293-7060
FACSIMILE (202) 293-7860
www.sughrue.com

December 26, 2000

J. Frank Osha, Esq.
Direct Dial (202) 663-7915
Email: fosha@sughrue.com

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Application of Masayuki TERAOK, Akira SAKAI, Masakatsu TAKIZAWA, and Shuuji YAMAGUCHI
COMMUNICATION DEVICE, COMMUNICATION DEVICE SET,
AUTHENTICATION METHOD AND METHOD OF WIRELESS-CONNECTING
TERMINALS
Our Ref. Q62445

Dear Sir:

Attached hereto is the application identified above including 92 sheets of the specification, claims, 29 sheets of formal drawings, the executed Assignment and PTO 1595 form, and the executed Declaration and Power of Attorney. Also enclosed is an Information Disclosure Statement with Form PTO-1449 and references.


The Government filing fee is calculated as follows:

Total claims	34 - 20	=	14	x	\$18.00	=	\$252.00
Independent claims	11 - 3	=	8	x	\$80.00	=	\$640.00
Base Fee							\$710.00
TOTAL FILING FEE							\$1602.00
Recordation of Assignment							\$40.00
TOTAL FEE							\$1642.00

Checks for the statutory filing fee of \$1602.00 and Assignment recordation fee of \$40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from December 27, 1999 based on Japanese Application No. 369706/99. The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: 
J. Frank Osha
Registration No. 24,625

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

Teras et al #3
Filed 12/26/00
Q 62445
10f1

1c843 U.S. PTO
09/745808
12/26/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年12月27日

出 願 番 号

Application Number:

平成11年特許願第369706号

出 願 人

Applicant(s):

日本電気株式会社

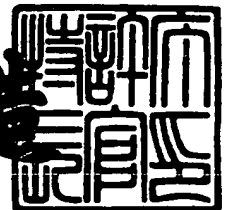
BEST AVAILABLE COPY

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 9月 8日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3072094

【書類名】 特許願

【整理番号】 62509030

【提出日】 平成11年12月27日

【あて先】 特許庁長官殿

【国際特許分類】 H04B 1/38

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 寺尾 正之

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 山口 修司

【発明者】

 【住所又は居所】 東京都港区高輪二丁目 2 0 番 3 6 号 株式会社エヌイー
シーデザイン内

 【氏名】 坂井 晃

【発明者】

 【住所又は居所】 東京都港区高輪二丁目 2 0 番 3 6 号 株式会社エヌイー
シーデザイン内

 【氏名】 滝澤 全克

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100088959

 【弁理士】

 【氏名又は名称】 境 廣巳

【手数料の表示】

 【予納台帳番号】 009715

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9002136

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信装置、通信装置セット、認証方法および端末間ワイヤレス接続方法

【特許請求の範囲】

【請求項 1】 端末装置のスロットに対して挿抜自在な通信装置であって、前記スロットに挿入されたときに端末装置から露出する部分が当該通信装置の種類に応じた色で色付けされている通信装置。

【請求項 2】 所定の移動体通信サービスに適合する無線部を有し、移動体通信サービスの種類に応じた色で色付けされている請求項 1 記載の通信装置。

【請求項 3】 特定のプロバイダーに接続するのに必要な情報が記憶された請求項 2 記載の通信装置。

【請求項 4】 端末装置のスロットに対して挿抜自在でそれぞれ異なる移動体通信サービスに適合する無線部を有する複数の通信装置のセットであって、前記スロットに挿入されたときに端末装置から露出する部分が各通信装置毎にそれぞれ異なる色で色付けされている通信装置セット。

【請求項 5】 端末装置のスロットに対して挿抜自在な通信装置と前記端末装置との間で認証を行う方法であって、

(a) 通信装置に記憶された ID と同じ ID を記憶させたキーモジュールをスロットに挿入し、該キーモジュールに記憶された ID を端末装置に登録するステップと、

(b) 端末装置とそのスロットに挿入された通信装置との間で、通信装置に記憶された ID と端末装置に登録された ID とが一致するか否かを照合するステップとを含む認証方法。

【請求項 6】 端末装置のスロットに対して挿抜自在な通信装置と前記端末装置との間で認証を行う方法であって、

(a) 通信装置に記憶された ID および認証コードと同じ ID および認証コードを記憶し且つ通信装置に記憶された逆暗号関数と対をなす暗号関数を記憶したキーモジュールをスロットに挿入し、該キーモジュールに記憶された ID、認証コード及び暗号関数を端末装置に登録するステップと、

(b) 通信装置がスロットに挿入されたとき、通信装置と端末装置との間で認証を行うステップとを含み、

前記ステップ b は、

(b-1) 通信装置に記憶された I D と端末装置に登録された I D とを照合するステップと、

(b-2) I D の照合が成功したときに、乱数を発生し、該乱数に認証コードを連結したものを暗号関数で暗号化したデータを端末装置から通信装置に送り、通信装置側では逆暗号関数によって認証コードと乱数を復元し、該復元した認証コードと記憶されている認証コードとを照合するステップと、

(b-3) 認証コードの照合が成功したときに、前記復元した乱数を逆暗号関数で暗号化したデータを通信装置から端末装置に送り、端末装置では暗号関数によって乱数を復元し、該復元した乱数と自ら生成した前記乱数とを照合するステップとを含む認証方法。

【請求項 7】 端末装置と通信装置との間で認証が成立した後、通信装置がスロットから取り出されたとき、端末装置を利用者からの入力を一切受け付けないロック状態とする請求項 5 または 6 記載の認証方法。

【請求項 8】 ロック状態の端末装置のスロットに通信装置が挿入されて端末装置と通信装置との間で認証が成立したとき、端末装置のロック状態を解除する請求項 7 記載の認証方法。

【請求項 9】 端末装置間をワイヤレス接続する通信装置であって、伝送速度に応じた色で色付けされている請求項 1 記載の通信装置。

【請求項 10】 端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在な複数の通信装置のセットであって、各通信装置は、自通信装置の通信アドレス及び同セット中の他の通信装置の通信アドレスを記憶する、前記端末装置から読み取り可能なメモリを備えた通信装置セット。

【請求項 11】 各通信装置の前記メモリに、データ暗号化用の共通鍵を記憶してある請求項 10 記載の通信装置セット。

【請求項 12】 各通信装置の前記メモリに、自通信装置の秘密鍵と同セット中の他の通信装置の公開鍵とを記憶してある請求項 10 記載の通信装置セット

【請求項 1 3】 端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在な複数の通信装置のセットであって、各通信装置は、自通信装置の通信アドレス及びデータ暗号化用のセット固有の共通鍵を記憶する、前記端末装置から読み取り可能なメモリを備えた通信装置セット。

【請求項 1 4】 端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在な複数の通信装置のセットであって、各通信装置は、自通信装置の通信アドレス、データ暗号化用の公開鍵およびデータ復号化用の秘密鍵を記憶する、前記端末装置から読み取り可能なメモリを備えた通信装置セット。

【請求項 1 5】 端末装置のスロットに挿入されたときに端末装置から一部はみ出る部分に通信装置固有の番号が付記されており、通信装置の通信アドレスは上位アドレス部と下位アドレス部とから構成され、前記番号が下位アドレス部に設定されている請求項 1 0 ないし 1 4 の何れかに記載の通信装置セット。

【請求項 1 6】 端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在であり且つ自通信装置の通信アドレスを記憶するメモリを備えた複数の通信装置のセットを使って、複数の端末装置間をローカルにワイヤレス接続する方法であって、

- (a) ワイヤレス接続する端末装置のそれぞれに通信装置を割り当てる段階、
- (b) 各通信装置を割り当て先の端末装置以外の端末装置のスロットに挿入し、その通信装置のメモリに記憶された通信アドレスを挿入先の端末装置の送信先一覧テーブルに登録する段階、
- (c) 各通信装置を割り当て先の端末装置のスロットに挿入する段階、
- (d) 送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用して、通信装置が挿入された端末装置間でデータを送受信する段階、

を含む端末間ワイヤレス接続方法。

【請求項 1 7】 各通信装置の前記メモリにセット固有の共通鍵を記憶し、送信データの暗号化および受信データの復号化に前記共通鍵を使用する請求項 1 6 記載の端末間ワイヤレス接続方法。

【請求項 1 8】 端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在であり且つ自通信装置の通信アドレス、公開鍵および秘密鍵を記憶するメモリを備えた複数の通信装置のセットを使って、複数の端末装置間をローカルにワイヤレス接続する方法であって、

- (a) ワイヤレス接続する端末装置のそれぞれに通信装置を割り当てる段階、
 - (b) 各通信装置を割り当て先の端末装置以外の端末装置のスロットに挿入し、その通信装置に記憶された通信アドレスおよび公開鍵を挿入先の端末装置の送信先一覧テーブルに登録する段階、
 - (c) 各通信装置を割り当て先の端末装置のスロットに挿入する段階、
 - (d) 送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化に送信先通信装置の公開鍵を使用し、受信データの復号化に秘密鍵を使用して、通信装置が挿入された端末装置間でデータを送受信する段階、
- を含む端末間ワイヤレス接続方法。

【請求項 1 9】 端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在であり且つ自通信装置の通信アドレスを記憶するメモリを備えた複数の通信装置のセットを使って、複数の端末装置間をローカルにワイヤレス接続する方法であって、

- (a) ワイヤレス接続する端末装置のそれぞれに通信装置を割り当てる段階、
- (b) 特定の端末装置のスロットに、他の端末装置に割り当てられた通信装置を順番に挿入し、その通信装置に記憶された通信アドレスを前記特定の端末装置の送信先一覧テーブルに登録する段階、
- (c) 各通信装置を割り当て先の端末装置のスロットに挿入する段階、
- (d) 前記特定の端末装置から他の端末装置に対して順番に、前記送信先一覧テーブルの内容を、今回の送信先通信装置の通信アドレス部分を前記特定の端末装置に挿入された通信装置に記憶された通信アドレスに置き換えて送信し、受信側各端末装置において受信した送信先一覧テーブルの内容を自装置の送信先一覧テーブルに設定する段階、
- (e) 送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装

置の通信アドレスを使用して、通信装置が挿入された端末装置間でデータを送受信する段階、

を含む端末間ワイヤレス接続方法。

【請求項 2 0】 各通信装置の前記メモリにセット固有の共通鍵を記憶し、送信データの暗号化および受信データの復号化に前記共通鍵を使用する請求項 1 9 記載の端末間ワイヤレス接続方法。

【請求項 2 1】 複数のスロットを有し且つスロット間のデータ中継機能を有する中継装置の 1 つのスロットに第 1 セットの通信装置を挿入し、他の 1 つのスロットに第 2 セットの通信装置を挿入し、第 1 セットの他の通信装置が挿入された端末装置と第 2 セットの他の通信装置が挿入された端末装置間を前記中継装置を介して通信可能とする請求項 1 6、1 7 または 2 0 記載の端末間ワイヤレス接続方法。

【請求項 2 2】 端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在であり且つ自通信装置の通信アドレス、公開鍵および秘密鍵を記憶するメモリを備えた複数の通信装置のセットを使って、複数の端末装置間をローカルにワイヤレス接続する方法であって、

- (a) ワイヤレス接続する端末装置のそれぞれに通信装置を割り当てる段階、
- (b) 特定の端末装置のスロットに、他の端末装置に割り当てられた通信装置を順番に挿入し、その通信装置に記憶された通信アドレスおよび公開鍵を前記特定の端末装置の送信先一覧テーブルに登録する段階、
- (c) 各通信装置を割り当て先の端末装置のスロットに挿入する段階、
- (d) 前記特定の端末装置から他の端末装置に対して順番に、前記送信先一覧テーブルの内容を、今回の送信先通信装置の通信アドレスおよび公開鍵の部分の前記特定の端末装置に挿入された通信装置に記憶された通信アドレスおよび公開鍵に置き換えて送信し、受信側端末装置において受信した送信先一覧テーブルの内容を自装置の送信先一覧テーブルに設定する段階、
- (e) 送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化に送信先通信装置の公開鍵を使用し、受信データの復号化に秘密鍵を使用して、通信装置が挿入された端末装置

間でデータを送受信する段階、
を含む端末間ワイヤレス接続方法。

【請求項 2 3】 端末装置のスロットに挿入されたときに端末装置から一部はみ出る部分に通信装置固有の番号が付記されており、通信装置の通信アドレスは上位アドレス部と下位アドレス部とから構成され、前記番号が下位アドレス部に設定されている請求項 1 6 ないし 2 2 の何れかに記載の端末間ワイヤレス接続方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は端末装置に対して挿抜自在な通信装置に関し、また通信装置と端末装置との間の認証方法および通信装置を使って端末間をワイヤレス接続する方法に関する。

【0 0 0 2】

【従来の技術】

端末装置に対して挿抜自在な通信装置は、従来より各種のものが提案されている。例えば特開平 8 - 1 4 9 0 3 5 号公報（以下、文献 1 と称す）では、情報端末とのインタフェース手段、アンテナ及び無線送受信回路を備え、情報端末の P C M C I A (P e r s o n a l C o m p u t e r M e m o r y C a r d I n t e r n a t i o n a l A s s o c i a t i o n) 規格のスロットに挿入して使用するカード型無線通信装置が提案されている。また同文献 1 には、カード型無線通信装置に、G S M (G l o b a l S y s t e m f o r M o b i l e c o m m u n i c a t i o n) システムの個々の加入者に交付される認証モジュールを装着する部位を設け、認証モジュールを装着したカード型無線通信装置を情報端末に挿入したときにユーザから暗証番号を入力させ、この入力された暗証番号と認証モジュールに事前に設定された暗証番号とを照合することにより、他人による悪用を防止する技術も示されている。

【0 0 0 3】

P C M C I A 規格のスロットなどに挿抜自在な通信装置としては、他に、特開

平 8 - 3 2 1 7 9 1 号公報（以下、文献 2 と称す）に記載されたデータ通信用無線トランシーバーや、特開平 1 1 - 1 5 4 8 8 6 号公報（以下、文献 3 と称す）に記載された無線端末がある。

【 0 0 0 4 】

【発明が解決しようとする課題】

端末装置に対して挿抜自在な通信装置は、文献 1 ～ 3 に示されるように従来より各種のものが提案されているが、以下のような課題があった。

【 0 0 0 5 】

（1）一般に移動体通信サービスには、GSM システム、CDMA（Code Division Multiple Access）システム、PDC（Personal Digital Cellular）システム、PHS（Personal Handyphone System）システムなど各種のものがある。このため、種々の無線インフラに対応するためには、それぞれの移動体通信サービスに対応した通信装置を用意し、通信装置を差し替えて使用が必要がある。この場合に問題となるのは、現在使っている通信装置がどの移動体通信サービスに対応するものであるかを、ユーザが即座に認知できないことである。その理由は前記各文献 1 ～ 3 では、移動体通信サービスとして或る特定のものを前提としているため、通信装置の種類をユーザに認知させる構成となっていないからである。

【 0 0 0 6 】

（2）文献 1 に記載のカード型無線通信装置では、他人による悪用を防止するために暗証番号を利用しているが、そのためにユーザは、カード型無線通信装置を異なる端末装置に装着する都度、暗証番号を入力する必要があり、利便性が阻害される。

【 0 0 0 7 】

（3）従来のこの種の通信装置は、移動体通信サービスの使用を前提としている。このため、各個人が所有する PDA（Personal Digital Assistant）、携帯電話、パーソナルコンピュータ（PC）などの各端末それぞれに通信装置を挿入し、通信装置間で通信することによって複数の端末間

をワイヤレス接続した場合、通信の都度、移動体通信サービスを利用しなければならない為に料金がかかり、また高速な通信が困難である。端末装置間をローカルに接続する技術に無線LANシステムがあるが、規模が大きく且つ通信アドレスの設定に専門的な知識が必要になるため、一般家庭では手軽に利用できない。

【0008】

本発明は以上のような事情に鑑みて提案されたものであり、その目的は、現在どのような通信装置を使用しているかをユーザが極めて容易に認知できるようにすることにある。

【0009】

本発明の別の目的は、他人による通信装置の悪用を防止するために必要なユーザの作業量を削減することにある。

【0010】

本発明の他の目的は、端末装置間を手軽にワイヤレス接続できるようにすることにある。

【0011】

【課題を解決するための手段】

本発明の通信装置および通信装置セットは、端末装置のスロットに挿入されたときに端末装置から露出する部分が通信装置の種類に応じた色で色付けされている。これによって、どの移動体通信サービス用の通信装置であるかが、スロットに挿入された状態でも外部から即座に認識することができる。移動体通信サービスとしては、例えばPHSシステム、PDCシステム、CDMAシステムが考えられるが、それらに限定されない。また、通信装置を購入すればインターネットのプロバイダーへの接続が行えるようにするために、各通信装置は、特定のプロバイダーに接続するのに必要な情報を記憶するメモリを備えるよう構成されていても良い。

【0012】

本発明の認証方法では、通信装置とは別にキーモジュールという部品を使う。キーモジュールは通信装置と同じ形をしており、端末装置のスロットに挿抜自在になっている。キーモジュールには、通信装置に記憶されたIDと同じIDが記

憶されており、通信装置を使用する予定の1つ或いは複数の端末装置のスロットに挿入して、IDをキーモジュールから端末装置側に登録する。IDを一旦登録したら、キーモジュールは持ち歩く必要はない。通信装置を端末装置のスロットに挿入して使用する際、端末装置と通信装置との間で、通信装置に記憶されたIDと端末装置に登録されたIDとが一致するか否かが調べられる。従来のようにユーザがパスワードを一々入力する必要がなく、ユーザの作業量が軽減される。また登録には必ずキーモジュールが必要であるため、パスワード入力より安全性が高い。IDの一致のみ照合するのではなく、以下のように、より厳格に相互認証するようにしても良い。

【0013】

キーモジュールに、通信装置に記憶されたIDおよび認証コードと同じIDおよび認証コードを記憶させておくと共に、通信装置に記憶された逆暗号関数と対をなす暗号関数を記憶させておき、それらを端末装置に登録し、通信装置がスロットに挿入されたとき、通信装置と端末装置との間で上記の各種のデータを用いて認証を行わせる。まず、通信装置に記憶されたIDと端末装置に登録されたIDとを照合する。次に、IDの照合が成功したときに、乱数を発生し、該乱数に認証コードを連結したものを暗号関数で暗号化したデータを端末装置から通信装置に送り、通信装置側では逆暗号関数によって認証コードと乱数を復元し、該復元した認証コードと記憶されている認証コードとを照合する。更に、認証コードの照合が成功したときに、前記復元した乱数を逆暗号関数で暗号化したデータを通信装置から端末装置に送り、端末装置では暗号関数によって乱数を復元し、該復元した乱数と自ら生成した前記乱数とを照合する。このように乱数を導入することにより、認証時に転送データが一意になるのを防止でき、悪意のある第三者に対して頑健な認証が実現できる。

【0014】

端末装置と通信装置との間で認証が成立した後、通信装置がスロットから取り出されたとき、端末装置を利用者からの入力を一切受け付けないロック状態としても良い。こうすれば通信装置に鍵（キー）の機能を持たせることができる。なお、ロック状態の端末装置のスロットに通信装置が挿入されて端末装置と通信装

置との間で認証が成立したとき、端末装置のロック状態は解除される。

【0015】

本発明の通信装置および通信装置セットは、また、端末装置間をワイヤレス接続する場合にも使用できる。その場合、伝送速度に応じた色で色付けされており、どの伝送速度のタイプであるかがスロットに挿入された状態でも外部から即座に認識することができるようになっている。

【0016】

本発明の端末間ワイヤレス接続用の通信装置セットの一例は、各通信装置が自通信装置の通信アドレス及び同セット中の他の通信装置の通信アドレスを記憶するメモリを備えている。また、データ暗号化用に共通鍵を使用する場合、その共通鍵もメモリに記憶され、データ暗号化用に公開鍵、復号化用に秘密鍵を使用する場合、各通信装置のメモリに自通信装置の秘密鍵と同セット中の他の通信装置の公開鍵とが事前に記憶されている。各通信装置に同セット中の他の通信装置の通信アドレスが記憶されているため、或る端末装置のスロットにその端末装置に割り当てた通信装置を挿入すれば、その端末装置はその通信装置から通信アドレス情報を読み出すだけで、自通信装置の通信アドレスおよび通信相手となる他の通信装置の通信アドレスを認識できる。この為、通信アドレスを設定する作業からユーザは解放され、また暗号化したデータを送受信する際の鍵も事前に設定されているため、鍵の設定をユーザ自身が行う必要がなくなる。

【0017】

本発明の端末間ワイヤレス接続用の通信装置セットの他の例は、各通信装置が同セットの他の通信装置の通信アドレスを記憶せず、自通信装置の通信アドレスだけを記憶している。このため、通信装置を使って複数の端末装置間をローカルにワイヤレス接続する場合、まず、ワイヤレス接続する端末装置のそれぞれに通信装置を割り当て、次に、各通信装置を割り当て先の端末装置以外の端末装置のスロットに挿入し、その通信装置のメモリに記憶された通信アドレスを挿入先の端末装置の送信先一覧テーブルに登録する。そして、各通信装置を割り当て先の端末装置のスロットに挿入し、以後、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用して、通信装置が挿入さ

れた端末装置間でデータを送受信する。

【0018】

勿論、各通信装置の前記メモリにセット固有の共通鍵を記憶しておき、送信データの暗号化および受信データの復号化に前記共通鍵を使用するようにしても良い。また、セット固有の共通鍵を使うと異なるセットの通信装置間では通信が行えない。それを可能にするには、複数のスロットを有し且つスロット間のデータ中継機能を有する中継装置を使用すれば良い。つまり、中継装置の1つのスロットに第1セットの通信装置を挿入し、他の1つのスロットに第2セットの通信装置を挿入し、第1セットの他の通信装置が挿入された端末装置と第2セットの他の通信装置が挿入された端末装置間を前記中継装置を介して通信可能とする。

【0019】

また、公開鍵、秘密鍵を使った暗号化方式によるデータ送信も可能である。この場合は、各通信装置のメモリに、自通信装置の通信アドレス、公開鍵および秘密鍵を記憶しておき、各通信装置を割り当て先の端末装置以外の端末装置のスロットに挿入し、その通信装置に記憶された通信アドレスおよび公開鍵を挿入先の端末装置の送信先一覧テーブルに登録する。そして、各通信装置を割り当て先の端末装置のスロットに挿入し、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化に送信先通信装置の公開鍵を使用し、受信データの復号化に秘密鍵を使用して、通信装置が挿入された端末装置間でデータを送受信する。

【0020】

上記の方法は、2つ或いは3つといった少数の端末装置間をワイヤレス接続するのに好適である。しかし、ワイヤレス接続する端末装置の数が増えると、通信装置のスロットへの挿入回数が増え、ユーザの作業量が増える。以下のような方法によれば、端末装置数が増えてもユーザの作業量を少なく抑えることができる。まず、特定の端末装置のスロットに、他の端末装置に割り当てられた通信装置を順番に挿入し、その通信装置に記憶された通信アドレスを前記特定の端末装置の送信先一覧テーブルに登録する。次に、各通信装置を割り当て先の端末装置のスロットに挿入し、前記特定の端末装置から他の端末装置に対して順番に、前記

送信先一覧テーブルの内容を、今回の送信先通信装置の通信アドレス部分を前記特定の端末装置に挿入された通信装置に記憶された通信アドレスに置き換えて送信し、受信側各端末装置において受信した送信先一覧テーブルの内容を自装置の送信先一覧テーブルに設定する。以後、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用して、通信装置が挿入された端末装置間でデータを送受信する。

【 0 0 2 1 】

勿論、各通信装置の前記メモリにセット固有の共通鍵を記憶しておき、送信データの暗号化および受信データの復号化に前記共通鍵を使用するようにしても良い。また、セット固有の共通鍵を使うと異なるセットの通信装置間では通信が行えないが、その場合には前述した中継装置を利用すれば良い。また、公開鍵、秘密鍵を使った暗号化方式によるデータ送信を行う場合は、各通信装置の前記メモリに自通信装置の通信アドレス、公開鍵および秘密鍵を記憶させておき、特定の端末装置のスロットに、他の端末装置に割り当てられた通信装置を順番に挿入し、その通信装置に記憶された通信アドレスおよび公開鍵を前記特定の端末装置の送信先一覧テーブルに登録する。次に、各通信装置を割り当て先の端末装置のスロットに挿入し、前記特定の端末装置から他の端末装置に対して順番に、前記送信先一覧テーブルの内容を、今回の送信先通信装置の通信アドレスおよび公開鍵の部分を前記特定の端末装置に挿入された通信装置に記憶された通信アドレスおよび公開鍵に置き換えて送信し、受信側端末装置において受信した送信先一覧テーブルの内容を自装置の送信先一覧テーブルに設定する。以後、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化に送信先通信装置の公開鍵を使用し、受信データの復号化に秘密鍵を使用して、通信装置が挿入された端末装置間でデータを送受信する。

【 0 0 2 2 】

また本発明の端末間ワイヤレス接続用の通信装置は、端末装置のスロットに挿入されたときに端末装置から一部はみ出る部分に通信装置固有の番号が付記されており、その通信装置の通信アドレスは上位アドレス部と下位アドレス部とから

構成され、前記番号が下位アドレス部に設定されている。これにより、ユーザは通信アドレスの下位アドレス部の値と通信装置に付記された番号とを見比べることによって、どの通信装置がどの通信アドレスに対応しているかを認識することができる。

【0023】

【発明の実施の形態】

次に本発明の実施の形態の例について図面を参照して詳細に説明する。

【0024】

図1を参照すると、本発明の一実施の形態は、携帯端末装置1a、PDA1b、PC（パーソナルコンピュータ）1cの3台の端末装置が、それぞれに設けられたスロット2a、2b、2cに挿入された通信装置3a、3b、3cによって相互にワイヤレス接続されている。通信装置3a～3cのそれぞれは、規格化された同一の外形形状を有し、また内部構造も全て同じになっている。通信装置3a～3cの構成例を図2に示す。

【0025】

図2を参照すると、コネクタ31は、装置筐体30の一端側に設けられており、通信装置がスロット内に挿入されたときに通信装置側に設けられたソケットと物理的かつ電氣的に結合する。アンテナ32は、コネクタ31と反対側の端部に設けられており、通信装置がスロットに装着された状態ではスロット外にはみ出る。アンテナ32はスロットアンテナ等の小型アンテナで構成される。コネクタ31とアンテナ32との間には、インタフェイス33、制御部34、メモリ35および無線部36が設けられる。インタフェイス33はコネクタ31と信号線L1で接続されると共に信号線L2で制御部34に接続され、制御部34は信号線L3、L4でメモリ35、無線部36に接続され、無線部36は信号線L5でアンテナ32に接続される。また、コネクタ31を通じて端末装置側から供給される電力が電源線37を介して各部に供給される構成となっている。

【0026】

メモリ35は、ROM等の不揮発性メモリで構成され、少なくとも自通信装置の通信アドレスを記憶している。メモリ35に記憶された通信アドレスは、通信

装置の起動時に制御部 3 4 で読み取られ、無線部 3 6 に対して自通信装置の通信アドレスとして設定される。また、メモリ 3 5 の記憶情報は、制御部 3 4、インタフェイス 3 3 およびコネクタ 3 1 を介して端末装置から読み取り可能になっている。

【 0 0 2 7 】

無線部 3 6 は、無線周波数信号を生成し、伝送し、受信する機能を持つ。この無線部 3 6 は、例えば IEEE 8 0 2 . 1 として標準化されている無線 LAN の規格に準拠した既存の無線 LAN システムにおける子機の無線部を流用して実現することができ、その場合、通信方式も直接拡散方式、周波数ホッピング方式など任意の方式を利用できる。また、bluetooth システムで使われる無線部を流用することもできる。使用する周波数帯は 2 . 4 G H z、4 G H z 等、種々のタイプがある。また、媒体アクセス制御機能を持たせるようにしても良い。その場合、例えば、送信前にキャリアをセンスし、キャリアを検出したら送信を行わず、ランダム時間後に再送信を試みる分散制御型の CSMA / CA (C a r r i e r S e n s e M u l t i p l e A c c e s s w i t h C o l l i s i o n A v o i d a n c e) が使用できる。

【 0 0 2 8 】

インタフェイス 3 3 は、コネクタ 3 1 と共に所定の電氣的ないし機械的規格に適合するアダプタを構成する。規格としては、例えば PCMCIA 規格を採用することができるが、USB (U n i v e r s a l S e r i a l B u s) などの他の規格であっても良い。

【 0 0 2 9 】

制御部 3 4 は、通信装置全体の制御を司る部分であり、例えば MPU 及び制御用プログラムを記憶する ROM 等で構成される。制御部 3 4 は、無線部 3 6 で受信された自通信装置宛のデータをインタフェイス 3 3 及びコネクタ 3 1 経由で端末装置に伝達する制御、端末装置側からコネクタ 3 1 及びインタフェイス 3 3 経由で伝達された送信データを無線部 3 6 に伝達して送信させる制御といった送受信にかかる基本的な制御機能に加え、各種の付加的な制御機能を有する。

【 0 0 3 0 】

携帯端末装置 1 a の構成例を図 3 に示す。図 3 を参照すると、携帯端末装置 1 a は、装置筐体 1 0 0 内に、キーパッド 1 0 1、LCD 等の表示器 1 0 2、アナログからデジタル及びその逆変換を行う A/D 変換器 1 0 3、これらと信号線 L 1 1 ~ L 1 3 で接続された制御部 1 0 4、A/D 変換器 1 0 3 に信号線 L 1 4 で接続されたマイク/スピーカ 1 0 5、制御部 1 0 4 に信号線 L 1 5 で接続されたメモリ 1 0 6、制御部 1 0 4 に信号線 L 1 6 で接続されたインタフェイス 1 0 7 及び各部に電力を供給する電源 1 0 8 を有し、またスロット 2 a を備え、このスロット 2 a 内に信号線 L 1 7 でインタフェイス 1 0 7 と接続されたソケット 1 0 9 が設けられている。

【0031】

ソケット 1 0 9 とインタフェイス 1 0 7 は、図 2 に示す通信装置 3 a ~ 3 c 側のアダプタ (3 1、3 3) に電氣的ないし機械的に適合するアダプタを構成する。A/D 変換器 1 0 3 は、マイクからのアナログ音声信号をデジタル音声信号へ変換し、制御部 1 0 4 からスピーカへ出力される音声信号をデジタル信号からアナログ信号へ変換する。制御部 1 0 4 は、一般の携帯電話が有する送受話制御機能に加えて、各種の付加的な機能を有し、例えば MPU 及び制御プログラムを記憶する ROM で構成される。メモリ 1 0 6 は、例えば RAM で構成され、各種のデータを記憶するために利用される。

【0032】

PDA 1 b の構成例を図 4 に示す。図 4 を参照すると、PDA 1 b は、装置筐体 1 1 0 内に、MPU 1 1 1 とそのバス 1 1 2 に接続された ROM 1 1 3、RAM 1 1 4、キーボードコントローラ 1 1 5、表示コントローラ 1 1 6、タブレットコントローラ 1 1 7 およびインタフェイス 1 1 8 と、キーボードコントローラ 1 1 5 に信号線 L 3 1 で接続されたキーボード 1 1 9 と、表示コントローラ 1 1 6 に信号線 L 3 2 で接続された LCD 等の表示器 1 2 0 と、タブレットコントローラ 1 1 7 に信号線 L 3 3 で接続されたタブレット 1 2 1 と、各部に電力を供給する電源 1 2 2 とを有し、またスロット 2 b を備え、このスロット 2 b 内に信号線 L 3 4 でインタフェイス 1 1 8 と接続されたソケット 1 2 3 が設けられている。

【0033】

ソケット123とインタフェース118は、通信装置3aから3c側のアダプタ(31、33)に電氣的ないし機械的に適合するアダプタを構成する。タブレット121は表示器120の表示面を覆うように配置されており、表示器120及びそれらのコントローラ116、117と共にペン入力機能付き表示装置を構成する。MPU111は、PDA1b全体の制御を司る制御部を構成し、ROM113はMPU111で実行する各種のプログラムを記憶する。RAM114は各種のデータを記憶するために利用される。

【0034】

PC1cは、PDA1bと基本的に同じ構成を有する。但し、ペン入力方式でないPCではタブレット121およびタブレットコントローラ117は省略される。また一般にマウス入力が可能であり、電源も通常は商用電源が利用される。

【0035】

次に、端末装置間をワイヤレス接続する実施例について説明する。

【0036】

【実施例1】

通信装置は複数本を1セットとしてユーザに販売される。含まれる通信装置の数の違いによって、また伝送速度の違いによって、様々なセットが存在する。例えば或るセットは、伝送速度2Mbpsの2個の通信装置から構成され、他のセットは伝送速度4Mbpsの10個の通信装置から構成される。各セット中の通信装置は、スロットに挿入されたときにスロット外にはみ出る部分に伝送速度に応じた色が塗られており、色によって通信装置の伝送速度が認識できるようになっている。例えば、2Mbpsは黄色、4Mbpsはオレンジ、10Mbpsは赤、16Mbpsは青、32Mbpsは緑である。なお、通信装置はスロット外にはみ出る必要は必ずしもなく、露出していれば良い。また、各セット中の通信装置には1から始まる連続番号が付記されている。価格は伝送速度が早くなれば高くなり、またセットに含まれる通信装置の個数が増えるほど高くなる。ユーザは、伝送速度と本数を決め、該当するセットを購入する。通信装置の個数は、ワイヤレス接続したい端末装置の総台数以上必要である。

【0037】

図5に、ユーザが購入した1セット分の通信装置の外観の概略を示す。この例のセットは3個組みのセットであり、通信装置3aには「1」、通信装置3bには「2」、通信装置3cには「3」がそれぞれ印刷ないし刻字されている。伝送速度を示す色は、1～3の数字が色付け数字とされるか、または背景が着色される。後者の場合、端部全面を着色しても良く、一部を着色しても良い。

【0038】

本実施例の場合、同じセットの各通信装置3a～3bのメモリ35には、図5に付記するように、自通信装置の通信アドレス、他通信装置の通信アドレス、データ送信時に使う暗号化用の共通鍵が予め記憶されている。通信アドレスは、複数ビットで構成される上位アドレス部と、数ビットで構成される下位アドレス部とから成り、上位アドレス部には当該セット固有のアドレスが設定され、下位アドレス部にはその通信装置に付記された連続番号の数値が設定されている。

【0039】

図5に示した3個の通信装置3a～3cを使って、図1に示した3台の端末装置1a～1cをワイヤレス接続する場合、各端末装置1a～1cにそれぞれ1個の通信装置3a～3cを割り当て、それぞれ登録作業を行う。以下、端末装置1aに通信装置3aを、端末装置1bに通信装置3bを、端末装置1cに通信装置3cをそれぞれ割り当てたものとして、本実施例における登録作業について説明する。

【0040】

携帯端末装置1aのキーパッド101を操作して、ワイヤレス接続用の通信装置の登録処理を起動すると、制御部104は、図6に示す処理を開始する。まず、表示器102に「スロットに通信装置を挿入して下さい」といったメッセージを表示する(S1)。これに応じてユーザがスロット2aに通信装置3aを挿入すると、携帯端末装置1aに内蔵の電源108からソケット109を通じて通信装置3aに電力が供給されて通信装置3aが動作可能状態になる。次に、制御部104は、インタフェース107、ソケット109および通信装置3aのコネクタ31、インタフェース33および制御部34を通じて、メモリ35に記憶され

た自通信装置 3 a の通信アドレス、他通信装置 3 b、3 c の通信アドレスおよび共通鍵 K を読み込む (S 2)。そして、自通信装置情報テーブルを生成し (S 3)、送信先一覧テーブルを生成し (S 4)、送信先選択画面を生成し (S 5)、登録完了メッセージを表示器 1 0 2 に表示し (S 6)、処理を終了する。それぞれ生成された自通信装置情報テーブル、送信先一覧テーブルおよび送信先選択画面は、メモリ 1 0 6 に保存される。

【0041】

ステップ S 3 で生成される自通信装置情報テーブルの内容例を図 7 (a) に示す。自通信装置情報テーブル 1 3 0 は、通信装置番号、通信アドレス、鍵の項目から構成される。通信アドレスには、自通信装置 3 a の通信アドレスが設定され、通信装置番号には、自通信装置 3 a の通信アドレスの下位アドレス部で示される数値、つまり通信装置 3 a に付記された番号 1 が設定される。鍵には、共通鍵 K が設定される。

【0042】

ステップ S 4 で生成される送信先一覧テーブルの内容例を図 7 (b) に示す。送信先一覧テーブル 1 3 1 は、他通信装置 3 b、3 c 毎のエントリで構成され、各エントリは通信装置番号、通信アドレス、鍵の項目を含む。通信アドレスには、他通信装置 3 b、3 c の通信アドレスが設定される。通信装置番号には、他通信装置 3 b、3 c の通信アドレスの下位アドレス部で示される数値、つまり他通信装置 3 b、3 c に付記された番号 2、3 が設定される。鍵には、共通鍵 K が設定される。

【0043】

ステップ S 5 で生成される送信先選択画面は、実際の送信時に送信先をユーザに選択させる際に使用する画面であり、その内容例を図 7 (c) に示す。同図に示されるように送信先選択画面は、送信先一覧テーブル 1 3 1 に設定された通信装置番号 2、3 をユーザに提示し、その何れかを選択させる画面である。

【0044】

図 6 に示したような登録作業を支援する機能は、PDA 1 b および PC 1 c の MPU 1 1 1 によっても提供されており、ユーザは PDA 1 b および PC 1 c に

対し通信装置 3 b、3 c を使用して携帯端末装置 1 a と同様な作業を繰り返す。これによって、PDA 1 b および PC 1 c の RAM 114 に、図 7 と同様な自通信装置情報テーブル、送信先一覧テーブルおよび送信先選択画面が生成される。但し、通信装置 3 a と通信装置 3 b、通信装置 3 c とでは、自通信装置、他通信装置が異なるので内容は同じでない。

【0045】

以上のような登録作業が完了すると、携帯端末装置 1 a、PDA 1 b、PC 1 c 間で相互にデータのワイヤレス送受信が可能となる。例えば携帯端末装置 1 a のメモリ 106 に記憶された或る種のファイル（例えば電話帳ファイル）を送信対象ファイルに選択し、図 7（c）に示した送信先選択画面で例えば 2 番を選択して、キーパッド 101 の操作で送信開始を指示すると、制御部 104 は、ワイヤレス送信制御を開始する。まず、送信対象ファイルをメモリ 106 から読み出し、自通信装置情報テーブル 130 に記憶されている共通鍵 K で暗号化する。そして、例えば図 8 に示すようなヘッダ 140、送信先アドレス 141、送信元アドレス 142、送信データ 143 及びそのパリティビット等のチェックビット 144 から構成されるフォーマットの送信データを生成し、インタフェース 107 を通じて通信装置 3 a に送り込む。ここで、送信先アドレス 141 は、送信先選択画面にてユーザが選択した番号に対応して送信先一覧テーブル 131 に記憶されている通信アドレスであり、送信元アドレス 142 は自通信装置情報テーブル 130 に記憶されている通信アドレスである。また、送信データ 143 は共通鍵 K で暗号化されている。通信装置 3 a の制御部 34 は、端末装置 1 a 側からの送信データをインタフェース 33 を介して受信すると、それを無線部 36 に送り込み、無線部 36 は無線周波数信号に変換し、アンテナ 32 から送信する。

【0046】

各端末装置 1 a ～ 1 b に挿入された各通信装置 3 a ～ 3 c における無線部 36 は、アンテナ 32 で受信されるデータの送信先アドレス 141 が自通信装置の通信アドレスと一致した場合、当該送信データを取り込み、制御部 34 に伝達する。制御部 34 は、この送信データをインタフェース 33 を通じて端末装置側に送り込む。例えば、送信先アドレス 141 に番号 2 の PDA 1 b に挿入された通信

装置 1 b の通信アドレスが設定されている場合、通信装置 3 a から送信されたデータは通信装置 3 b で受信され、PDA 1 b に送り込まれる。PDA 1 b の MPU 1 1 1 は、データをインタフェース 1 1 8 を通じて受け取り、チェックビット 1 4 4 によるチェックを行った後、誤りがなければ送信データ 1 4 3 を自通信情報テーブルに設定された共通鍵で復号化する。復号化されたデータは例えばその送信元アドレスと共に RAM 1 1 4 の受信エリアに格納され、その後、PDA 1 b のユーザにデータの受信を知らせるメッセージが表示器 1 2 0 に表示される。

【0047】

以上は携帯端末装置 1 a から PDA 1 b へのワイヤレス送信であるが、PDA 1 b から携帯端末装置 1 a や PC 1 c へのワイヤレス送信等、任意の装置間でも同様なワイヤレス送信が可能である。

【0048】

【実施例 2】

本実施例では、暗号化用の鍵として、通信装置固有の公開鍵を使用し、その復号に秘密鍵を使用する点で実施例 1 と相違し、その他の点は実施例 1 と同じである。図 9 に、ユーザが購入した 1 セット分の通信装置の外観の概略を示す。この例のセットは 3 個組みのセットであり、各通信装置 3 a ~ 3 b のメモリ 3 5 には、自通信装置の通信アドレス、他通信装置の通信アドレス、自通信装置の秘密鍵、他通信装置の公開鍵が予め記憶されている。図 9 に示した 3 個の通信装置 3 a ~ 3 c を使って、図 1 に示した 3 台の端末装置 1 a ~ 1 c をワイヤレス接続する場合、実施例 1 と同様な登録作業を行う。このとき図 6 のステップ S 2 では、自通信装置および他通信装置の通信アドレスと、自通信装置の秘密鍵と、他通信装置の公開鍵とが読み込まれ、図 7 の自通信装置情報テーブル 1 3 0 の鍵の項目に自通信装置の秘密鍵が設定され、送信先一覧テーブル 1 3 1 の鍵の項目には他通信装置の公開鍵が設定される。送信元の端末装置では、送信先端末装置の通信装置の公開鍵を使ってデータを暗号化して送信し、受信側の端末装置では自通信装置の秘密鍵を使って復号化する。

【0049】

【実施例 3】

本実施例では、暗号化用の鍵として、通信装置固有の公開鍵を使用し、その復号に秘密鍵を使用する点、それぞれの通信装置は自通信装置の通信アドレス、公開鍵および秘密鍵を記憶し、他通信装置の通信アドレス、公開鍵および秘密鍵は記憶していない点で実施例 1 と相違し、その他の点は実施例 1 と同じである。図 1 0 に、ユーザが購入した 1 セット分の通信装置の外観の概略を示す。この例のセットは 3 個組みのセットであり、各通信装置 3 a ~ 3 b のメモリ 3 5 には、自通信装置の通信アドレス、自通信装置の秘密鍵および公開鍵が予め記憶されている。

【 0 0 5 0 】

図 1 0 に示した 3 個の通信装置 3 a ~ 3 c を使って、図 1 に示した 3 台の端末装置 1 a ~ 1 c をワイヤレス接続する場合、各端末装置 1 a ~ 1 c にそれぞれ 1 個の通信装置 3 a ~ 3 c を割り当て、所定の登録作業を行う。以下、端末装置 1 a に通信装置 3 a を、端末装置 1 b に通信装置 3 b を、端末装置 1 c に通信装置 3 c をそれぞれ割り当てたものとして、本実施例における登録作業について説明する。

【 0 0 5 1 】

先ず、各端末装置 1 a ~ 1 c に自通信装置 3 a ~ 3 c の通信アドレス、秘密鍵及び公開鍵を登録する作業を説明する。

【 0 0 5 2 】

携帯端末装置 1 a のキーパッド 1 0 1 を操作して、ワイヤレス接続用の自通信装置の登録処理を起動すると、制御部 1 0 4 は、図 1 1 に示す処理を開始する。先ず、表示器 1 0 2 に「スロットに自通信装置を挿入して下さい」といったメッセージを表示する (S 1 1) 。これに応じてユーザがスロット 2 a に自通信装置 3 a を挿入すると、携帯端末装置 1 a に内蔵の電源 1 0 8 からソケット 1 0 9 を通じて通信装置 3 a に電力が供給されて通信装置 3 a が動作可能状態になる。次に、制御部 1 0 4 は、インタフェイス 1 0 7、ソケット 1 0 9 および通信装置 3 a のコネクタ 3 1、インタフェイス 3 3 および制御部 3 4 を通じて、メモリ 3 5 に記憶された自通信装置 3 a の通信アドレス、自通信装置 3 a の秘密鍵および公開鍵を読み込む (S 1 2) 。そして、自通信装置情報テーブルを生成し (S 1 3

）、登録完了メッセージを表示器 1 0 2 に表示し（S 1 4）、処理を終了する。
生成された自通信装置情報テーブルは、メモリ 1 0 6 に保存される。

【 0 0 5 3 】

ステップ S 1 3 で生成される自通信装置情報テーブルの内容例を図 1 2（a）に示す。自通信装置情報テーブル 1 4 0 は、通信装置番号、通信アドレス、鍵の項目から構成される。通信アドレスには、自通信装置 3 a の通信アドレスが設定され、通信装置番号には、自通信装置 3 a の通信アドレスの下位アドレス部で示される数値、つまり通信装置 3 a に付記された番号 1 が設定される。鍵には、自通信装置 3 a の秘密鍵および公開鍵が設定される。

【 0 0 5 4 】

図 1 1 に示したような自通信装置に関する登録作業を支援する機能は、PDA 1 b および PC 1 c の MPU 1 1 1 によっても提供されており、ユーザは PDA 1 b および PC 1 c に対し通信装置 3 b、3 c を使って携帯端末装置 1 a と同様な作業を繰り返す。これによって、PDA 1 b および PC 1 c の RAM 1 1 4 に、図 7（a）と同様な自通信装置情報テーブルが保存される。但し、通信装置 3 a と通信装置 3 b、通信装置 3 c とでは、通信アドレス、秘密鍵、公開鍵が異なるので内容は同じでない。

【 0 0 5 5 】

次に、各端末装置 1 a ～ 1 c に対して、他の端末装置に割り当てた通信装置 3 a ～ 3 c の通信アドレスおよび公開鍵を登録する作業について説明する。

【 0 0 5 6 】

携帯端末装置 1 a のキーパッド 1 0 1 を操作して、ワイヤレス接続用の他通信装置の登録処理を起動すると、制御部 1 0 4 は、図 1 3 に示す処理を開始する。まず、表示器 1 0 2 に「スロットに他通信装置を挿入して下さい」といったメッセージを表示する（S 3 1）。これに応じてユーザがスロット 2 a に例えば通信装置 3 b を挿入すると、携帯端末装置 1 a に内蔵の電源 1 0 8 によって通信装置 3 b が動作可能状態になる。次に、制御部 1 0 4 は、インタフェース 1 0 7、ソケット 1 0 9 および通信装置 3 a のコネクタ 3 1、インタフェース 3 3 および制御部 3 4 を通じて、メモリ 3 5 に記憶された通信装置 3 b の通信アドレス、通信

装置 3 a の公開鍵を読み込み、メモリ 1 0 6 に一時的に保持する (S 3 2)。次に制御部 1 0 4 は他通信装置が他にあるか否かを表示器 1 0 2 にメッセージを表示してユーザに問い合わせ、他の通信装置がある場合 (S 3 3 で N O)、ステップ S 3 1 に戻って上述した処理を繰り返す。今の場合、通信装置 3 c が残っているので、ユーザが通信装置 3 b に代えて通信装置 3 c をスロット 2 a に挿入すると、通信装置 3 c の通信アドレス、公開鍵が読み込まれ、メモリ 1 0 6 に一次的に保持される。

【 0 0 5 7 】

他通信装置 3 b、3 c の通信アドレス及び公開鍵を携帯端末装置 1 a に登録し終え、ユーザが他通信装置の終了をキーパッド 1 0 1 から入力すると (ステップ S 3 3 で Y E S)、制御部 1 0 4 は、送信先一覧テーブルを生成し (S 3 4)、送信先選択画面を生成し (S 3 5)、登録完了メッセージを表示器 1 0 2 に表示し (S 3 6)、処理を終了する。生成された送信先一覧テーブル、送信先選択画面は、メモリ 1 0 6 に保存される。

【 0 0 5 8 】

ステップ S 3 4 で生成される送信先一覧テーブルの内容例を図 1 2 (b) に示す。送信先一覧テーブル 1 4 1 は、他通信装置 3 b、3 c 毎のエントリで構成され、各エントリは通信装置番号、通信アドレス、鍵の項目を含む。通信アドレスには、他通信装置 3 b、3 c の通信アドレスが設定される。通信装置番号には、他通信装置 3 b、3 c の通信アドレスの下位アドレス部で示される数値、つまり他通信装置 3 b、3 c に付記された番号 2、3 が設定される。鍵には、通信装置 3 b、3 c の公開鍵が設定される。

【 0 0 5 9 】

ステップ S 3 5 で生成される送信先選択画面は、図 1 2 (c) に示すように、図 7 (c) に示したものと同一である。

【 0 0 6 0 】

図 1 3 に示したような他通信装置の登録作業を支援する機能は、P D A 1 b および P C 1 c の M P U 1 1 1 によっても提供されており、ユーザは P D A 1 b および P C 1 c に対して携帯端末装置 1 a と同様な作業を繰り返す。これによって

、PDA 1 b および PC 1 c の RAM 1 1 4 に、図 1 2 と同様な送信先一覧テーブルおよび送信先選択画面が保存される。但し、PDA 1 b には通信装置 3 a と通信装置 3 c の通信アドレス及び公開鍵が登録され、PC 1 c には通信装置 3 a と通信装置 3 b の通信アドレス及び公開鍵が登録されるので、内容は同じでない。

【0061】

以上のような登録作業が完了すると、実施例 1 と同様に携帯端末装置 1 a、PDA 1 b、PC 1 c 間で相互にデータのワイヤレス送受信が可能となる。

【0062】

本実施例では、携帯端末装置 1 a、PDA 1 b、PC 1 c を相互にワイヤレス接続したが、そのような構成に限定されない。例えば、携帯端末装置 1 a と PDA 1 b との間の接続が不要であれば、携帯端末装置 1 a には他通信装置として PC 1 c の通信装置 3 c のみを登録し、PDA 1 b には他通信装置として携帯端末装置 1 a の通信装置 3 a のみを登録すれば良い。

【0063】

【実施例 4】

本実施例では、ワイヤレス接続しようとする複数の端末装置のうちの何れか 1 つを情報配信サーバとし、サーバから他の全ての端末装置に対して送信先一覧テーブルを配信するようにした点で実施例 3 と相違し、その他の点は実施例 1 と同じである。本実施例の場合、図 1 0 に示した 3 個の通信装置 3 a ~ 3 c をそれぞれ割り当て先の端末装置 1 a、1 b、1 c のスロットに挿入して、各端末装置 1 a ~ 1 c の自通信装置情報テーブルに図 1 2 (a) に示したような自通信装置 3 a ~ 3 c の通信アドレス、秘密鍵及び公開鍵を登録した後、例えば端末装置 1 a を情報配信サーバとして、各端末装置 1 a ~ 1 c に、他の端末装置に割り当てた通信装置 3 a ~ 3 c の通信アドレスおよび公開鍵を登録する作業を行う。

【0064】

携帯端末装置 1 a のキーパッド 1 0 1 を操作して、ワイヤレス接続用の他通信装置の登録処理を起動すると、制御部 1 0 4 は、図 1 4 に示す処理を開始する。ステップ S 3 1 からステップ S 3 5 までは実施例 3 と同じ処理であり、図 1 2 (

b)、(c)に示したような送信先一覧テーブル141および送信先選択画面142が端末装置1aに生成される。続いて制御部104は、各端末装置にそれに割り当てた通信装置を挿入するよう促すメッセージを表示器102に表示する(S37)。ユーザは、このメッセージに従ってスロットへの通信装置の挿入作業を行う。

【0065】

次に制御部104は、送信先一覧テーブル141から1つの他通信装置、例えば通信装置3bを選択し(S38)、送信先一覧テーブル141中の当該選択した通信装置3bにかかる通信装置番号、通信アドレス、公開鍵を、自通信装置情報テーブル140中の自通信装置3aにかかる通信装置番号、通信アドレス、公開鍵で置き換えた配信用の送信先一覧テーブルを生成する(S40)。そして、この送信先一覧テーブルを、自装置1aのスロット2aに挿入された通信装置3aを使って、前記選択した通信装置3bがスロット2aに挿入されたPDA1bに送信する(S41)。この送信では、送信先アドレスに通信装置3bの通信アドレスを設定する。また、送信先一覧テーブルは通信装置3bの公開鍵で暗号化しておく。

【0066】

PDA1bのスロット2bに挿入された通信装置3bは、上記の配信データを受信すると、それをPDA1bに伝達し、PDA1bのMPU111は、自通信装置3bの秘密鍵で復号化し、得られた送信先一覧テーブルをRAM114に記憶する。また、送信先一覧テーブルに登録された通信装置番号に基づき送信先選択画面を生成し、RAM114に記憶する。

【0067】

携帯端末装置1aの制御部104は、PDA1bに対する配信を終えると、次に通信装置3cを選択し(S38)、送信先一覧テーブル141中の当該選択した通信装置3cにかかる通信装置番号、通信アドレス、公開鍵を、自通信装置情報テーブル140中の自通信装置3aにかかる通信装置番号、通信アドレス、公開鍵で置き換えた配信用の送信先一覧テーブルを生成し(S40)、PC1cに送信する(S41)。PC1cのスロット2cに挿入された通信装置3cは、上

記の配信データを受信すると、それを P C 1 c に伝達し、P C 1 c の M P U 1 1 1 は、自通信装置 3 c の秘密鍵で復号化し、得られた送信先一覧テーブルを R A M 1 1 4 に記憶する。また、送信先一覧テーブルに登録された通信装置番号に基づき送信先選択画面を生成し、R A M 1 1 4 に記憶する。

【0068】

携帯端末装置 1 a の制御部 1 0 4 は、送信先一覧テーブル 1 4 1 に未処理の通信装置が残っていないことを確認し（S 3 9 で Y E S）、登録完了メッセージを表示して（S 3 6）、処理を終える。

【0069】

【実施例 5】

本実施例は、実施例 3 と実施例 4 とを組み合わせたものである。つまり、実施例 3 の構成によってワイヤレス接続された複数の端末装置の何れかを情報配信サーバに設定して、新たな通信相手の登録を実施例 4 の構成によって実現するものである。例えば図 1 5 に示すように、無線でワイヤレス接続された通信装置 A 1、A 2、A 0 と、同じく無線でワイヤレス接続された通信装置 C 0、C 1 と、同じく無線でワイヤレス接続された通信装置 E 0、E 1 との 3 つのグループがある状況の下で、新たな通信装置 B 0、D 0 を導入し、通信装置 A 0、B 0、C 0、D 0、E 0 を相互にワイヤレス接続する場合について、本実施例の動作を説明する。なお、説明の便宜上、通信装置 A 0 は携帯端末装置 1 a に挿入された通信装置 3 a とする。

【0070】

先ず、実施例 4 と同様にして、新たな通信装置 B 0、D 0 の通信アドレス、秘密鍵及び公開鍵を、それらが割り当てられた端末装置に登録する。

【0071】

次に、携帯端末装置 1 a のキーパッド 1 0 1 を操作して、ワイヤレス接続用の他通信装置の追加処理を起動すると、制御部 1 0 4 は、図 1 6 に示す処理を開始する。先ず、表示器 1 0 2 に「スロットに追加する他通信装置を挿入して下さい」といったメッセージを表示する（S 5 1）。これに応じてユーザがスロット 2 a に例えば通信装置 B 0 を挿入すると、携帯端末装置 1 a に内蔵の電源 1 0 8 に

よって通信装置 B 0 が動作可能状態になる。次に、制御部 1 0 4 は、インタフェース 1 0 7、ソケット 1 0 9 および通信装置 B 0 のコネクタ 3 1、インタフェース 3 3 および制御部 3 4 を通じて、メモリ 3 5 に記憶された通信装置 B 0 の通信アドレス、通信装置 B 0 の公開鍵を読み込み、メモリ 1 0 6 に一時的に保持する (S 5 2)。次に制御部 1 0 4 は他通信装置が他にあるか否かを表示器 1 0 2 にメッセージを表示してユーザに問い合わせ、他の通信装置がある場合、ステップ S 5 1 に戻って上述した処理を繰り返す。今の場合、通信装置 D 0、C 0、E 0 が残っているので、ユーザが通信装置 B 0 に代えて順次にそれらの通信装置をスロット 2 a に挿入すると、各通信装置の通信アドレス、公開鍵が読み込まれ、メモリ 1 0 6 に一次的に保持される。

【 0 0 7 2 】

通信装置 B 0、D 0、C 0、E 0 の通信アドレス及び公開鍵を携帯端末装置 1 a に登録し終え、ユーザが追加他通信装置の終了をキーパッド 1 0 1 から入力すると (S 5 3 で Y E S)、制御部 1 0 4 は、サーバ用送信先一覧テーブルを生成し (S 5 4)、既にメモリ 1 0 6 に生成済の送信先一覧テーブルおよび送信先選択画面を更新する (S 5 5、S 5 6)。ここで、サーバ用送信先一覧テーブルは、追加された通信装置 B 0、D 0、C 0、E 0 の通信装置番号、通信アドレス、公開鍵を設定したテーブルである。また、送信先一覧テーブルおよび送信先選択画面には、サーバ用送信先一覧テーブルに設定された通信装置の情報が追加される。

【 0 0 7 3 】

続いて制御部 1 0 4 は、各端末装置にそれに割り当てた通信装置を挿入するよう促すメッセージを表示器 1 0 2 に表示する (S 5 7)。ユーザは、このメッセージに従ってスロットへの通信装置の挿入作業を行う。

【 0 0 7 4 】

次に制御部 1 0 4 は、サーバ用送信先一覧テーブルから 1 つの他通信装置、例えば通信装置 B 0 を選択し (S 5 8)、サーバ用送信先一覧テーブル中の当該選択した通信装置 B 0 にかかる通信装置番号、通信アドレス、公開鍵を、自通信装置情報テーブル中の自通信装置 A 0 にかかる通信装置番号、通信アドレス、公開

鍵で置き換えた配信用の送信先一覧テーブルを生成する（S60）。そして、この送信先一覧テーブルを、自装置のスロット2aに挿入された通信装置A0を使って、前記選択した通信装置B0がスロットに挿入された端末装置に送信する（S61）。この送信では、送信先アドレスに通信装置B0の通信アドレスを設定する。また、送信先一覧テーブルは通信装置B0の公開鍵で暗号化しておく。

【0075】

通信装置B0は、上記の配信データを受信すると、それをスロットを通じて端末装置に伝達し、端末装置の制御部は、自通信装置B0の秘密鍵で復号化し、得られた送信先一覧テーブルをメモリに記憶する。また、送信先一覧テーブルに登録された通信装置番号に基づき送信先選択画面を生成し、メモリに記憶する。

【0076】

携帯端末装置1aの制御部104は、通信装置B0に対する配信を終えると、同様の処理を通信装置D0、通信装置C0、通信装置E0に対して行う。通信装置D0側では通信装置B0と同じ動作が行われ、また通信装置C0、E0では、送信先一覧テーブルおよび送信先選択画面が既に作成されているので、送られてきた情報でそれらを更新する。制御部104は、通信装置B0、D0、C0、E0に対する配信を終えると、登録完了メッセージを表示し（S62）、処理を終える。

【0077】

以上のような登録作業が完了することにより、通信装置A0、B0、C0、D0、E0相互の通信が可能になる。但し、通信装置B0から通信装置A1、A2、C1、E1、通信装置C0から通信装置A1、A2、E1、通信装置D0から通信装置A1、A2、C1、E1、通信装置E0から通信装置A1、A2、C1へは、それぞれ通信できない。

【0078】

【実施例6】

本実施例では、中継装置を使って異なるセットの通信装置間での通信を実現する。その構成例を図17に示す。端末装置150～152はそれぞれのスロットに挿入された通信装置A0～A3によって相互にワイヤレス接続されている。ま

た、端末装置 1 6 0 ~ 1 6 2 はそれぞれのスロットに挿入された通信装置 F 0 ~ F 3 によって相互にワイヤレス接続されている。ここで、通信装置 A 0 ~ A 3 は同じセットの通信装置であり、共通鍵として K 1 を使用する。他方、通信装置 F 0 ~ F 3 も同じセットの通信装置であり、共通鍵として K 2 を使用する。共通鍵が異なるので、端末装置 1 5 0 と端末装置 1 6 0 とは直接に通信することはできない。中継装置 1 7 0 は、このような異なるセット間の通信を中継する装置であり、2 つのスロット 1 7 1、1 7 2 を持ち、またソケット 1 7 3、インタフェース 1 7 4、制御部 1 7 5、メモリ 1 7 6 を備えている。

【0079】

先ず、実施例 3 で説明した方法によって、スロット 1 7 1 に通信装置 A 0 と同じセット内の通信装置 A 3 を挿入して、メモリ 1 7 6 上に、図 1 8 (a) に示すような通信装置 A 3 の番号、通信アドレス、共通鍵 K 1 を持つ、スロット 1 7 1 対応の自通信装置情報テーブル 1 8 0 を生成し、また、通信装置 A 0 をスロット 1 7 1 に挿入して、メモリ 1 7 6 上に、図 1 8 (b) に示すような通信装置 A 0 の番号、通信アドレス、共通鍵 K 1 を持つ、スロット 1 7 1 対応の送信先情報テーブル 1 8 1 を生成する。更に、端末装置 1 5 0 の送信先一覧テーブルに通信装置 A 3 の通信装置番号、通信アドレス、共通鍵 K 1 を登録しておく。スロット 1 7 2 側についても同様の作業を行う。つまり、スロット 1 7 2 に通信装置 F 0 と同じセット内の通信装置 F 3 を挿入して、メモリ 1 7 6 上に、図 1 8 (c) に示すような通信装置 F 3 の番号、通信アドレス、共通鍵 K 2 を持つ、スロット 1 7 2 対応の自通信装置情報テーブル 1 8 2 を生成し、また、通信装置 F 0 をスロット 1 7 2 に挿入して、メモリ 1 7 6 上に、図 1 8 (d) に示すような通信装置 F 0 の番号、通信アドレス、共通鍵 K 2 を持つスロット 1 7 2 対応の送信先情報テーブル 1 8 3 を生成する。更に、端末装置 1 6 0 の送信先一覧テーブルに通信装置 F 3 の通信装置番号、通信アドレス、共通鍵 K 2 を登録しておく。これにより、通信装置 A 0 と通信装置 A 3 との間がワイヤレス接続され、また通信装置 F 0 と通信装置 F 3 との間がワイヤレス接続される。

【0080】

さて、通信装置 A 0 を持つ端末装置 1 5 0 から共通鍵 K 1 で暗号化されたデー

タが通信装置 A 3 に送信されてくると、中継装置 170 の制御部 175 は、スロット 171 対応の自通信装置情報テーブル 180 の共通鍵 K 1 によって暗号データを復号化し、スロット 172 対応の自通信装置情報テーブル 182 の共通鍵 K 2 によって再び暗号化する。そして、その暗号化したデータに、送信元アドレスとしてスロット 172 対応の自通信装置情報テーブル 182 の通信アドレスを、送信先アドレスとしてスロット 172 対応の送信先情報テーブル 183 の通信アドレスを、それぞれ付加した送信データを通信装置 F 2 によって、通信装置 F 0 に送信する。このデータを受信した通信装置 F 0 を持つ端末装置 160 は共通鍵 K 2 で復号化する。これとは逆の中継も同様に行われる。

【0081】

以上は中継専用の装置 170 を用いて異なるセットの通信装置間の接続を可能にしたが、端末装置自体に 2 つ以上のスロットと中継機能を持たせるようにしても良い。

【0082】

なお、以上の各実施例では、通信装置に固有の番号を付記し、その通信装置の通信アドレスの下位アドレス部に前記番号を設定し、送信先選択画面でその番号を表示することで、どの通信装置がどの端末装置に挿入されているかをユーザに認識させた。しかし、このような方法に代えて、例えば、各端末装置に自通信装置の通信アドレス及び他通信装置の通信アドレスを登録した後、各端末装置が他通信装置の通信アドレスを送信先アドレス、自通信装置の通信アドレスを送信元アドレスに指定して、他の端末装置に装置名を問い合わせるメッセージを送信し、このメッセージを受信した端末装置が自端末装置の名前（例えば携帯端末装置であるとか、PDA であるとか等）を返信し、この名前を前記番号に代えて、或いは番号と共に送信先選択画面に表示するようにしても良い。

【0083】

【発明の他の実施の形態】

これまでは、図 1 の携帯端末装置 1 a、PDA 1 b、PC 1 c をワイヤレス接続する構成について説明した。以下では、図 1 の携帯端末装置 1 a、PDA 1 b、PC 1 c から移動体通信サービスを利用する際の構成例について説明する。

【 0 0 8 4 】

図 1 9 は移動体通信サービスを利用する際に使用する通信装置のセットを示し、4 a は P H S システム用、5 a は P D C システム用、6 a は C D M A システム用の通信装置（以下、無線モジュールと称す）であり、それぞれ移動体通信システムを利用する際に端末装置のスロットに挿入して使用する。また、4 b、5 b、6 b は、正規の無線モジュールが正規の端末装置以外で不正に使用されるのを防止するための認証用のキーモジュールであり、無線モジュール 4 a、5 a、6 a に 1 対 1 に対応している。全ての無線モジュールおよびキーモジュールは、前述したワイヤレス接続用の通信装置と同じ規格で統一された同一の外形形状を有する。更に、無線モジュール 4 a、5 a、6 a は、端末装置のスロットに挿入したときに装置外にはみ出る装置の一部分（図 1 9 でハッチングを施した部分）が、利用できる移動体通信サービスの種類に応じた色で色付けされており、色を見れば、どの移動体通信サービス用の無線モジュールであるかが即座に認識できるようになっている。なお、無線モジュール 4 a、5 a、6 a はスロット外にはみ出る必要は必ずしもなく、露出していても良い。

【 0 0 8 5 】

無線モジュール 4 a、5 a、6 a の構造は、図 2 に示したワイヤレス接続用の通信装置 3 a ～ 3 c と基本的に同じであり、図 2 0 に示すように、筐体 3 0 の両端にコネクタ 3 1 およびアンテナ 3 2 を有し、筐体 3 0 内に、インタフェース 3 3、制御部 3 4、メモリ 3 5、無線部 3 6 および要素間を接続する信号線 L 1 ～ L 5 並びに電源線 3 7 を有している。但し、無線部 3 6 は、無線モジュール 4 a にあっては P H S システムに適合するよう設計され、無線モジュール 5 a にあっては P D C システムに適合するよう設計され、無線モジュール 6 a にあっては C D M A システムに適合するよう設計されている。また、メモリ 3 5 は E E P R O M 等の不揮発性メモリで構成され、何れも所定の認証用データが記憶されていると共に、P H S や P D C の場合は課金コードも記憶されている。

【 0 0 8 6 】

またキーモジュール 4 b、5 b、6 b は、図 2 1 に示すように、筐体 4 0 の一端にコネクタ 4 1 を有し、筐体 4 0 内に、コネクタ 4 1 に信号線 L 4 1 で接続さ

れたインタフェース 4 2、これに信号線 L 4 2 で接続された制御部 4 3、これに信号線 L 4 3 で接続されたメモリ 4 4 を有している。また、コネクタ 4 1 を通じて端末装置側から供給される電力を各部に伝達する電源線 4 5 がある。メモリ 4 4 は認証に使用する所定の情報を記憶する E E P R O M 等の不揮発性メモリである。コネクタ 4 1 とインタフェース 4 2 は、端末装置側のアダプタと機械的ないし電氣的に接続するアダプタを構成する。制御部 4 3 は M P U および制御プログラムを記憶する R O M 等で構成され、所定の認証処理を実行する。

【 0 0 8 7 】

例えば図 1 の携帯端末装置 1 a を P H S 電話機として利用する場合、P H S 用の無線モジュール 4 a と組になっているキーモジュール 4 b をスロット 2 a に挿入して、メモリ 4 4 に記憶されている認証用のデータを携帯端末装置 1 a 側に登録しておく。そして実際の利用時は、P H S 用の無線モジュール 4 a をスロット 2 a に挿入して P H S システムを利用する。このとき、無線モジュール 4 a と携帯端末装置 1 a との間で相互に認証が行われる。認証が成功しない限り、無線モジュール 4 a は使用できない。携帯端末装置 1 a を P D C 電話機、C D M A 電話機として利用することもできる。その場合も、事前にキーモジュール 5 b、6 b に記憶された認証用データを携帯端末装置 1 a 側に登録し、無線モジュール 5 a、6 a をスロット 2 a に挿入した際、無線モジュール 5 a、6 a と携帯端末装置 1 a とで相互に認証処理を行う。携帯端末装置 1 a と同様の作業を行えば、無線モジュール 4 a、5 a、6 a およびキーモジュール 4 b、5 b、6 b を使って P D A 1 b や P C 1 c で、P H S システム、P D A システム、C D M A システムを利用することもできる。

【 0 0 8 8 】

キーモジュール 4 b、5 b、6 b は、それを使って認証用のデータを端末装置に一旦登録してしまえば普段は使わない。したがってキーモジュール 4 b、5 b、6 b を厳重に保管しておけば、P H S、P D C、C D M A システム用の無線モジュール 4 a、5 a、6 a が盗難にあっても、悪用される心配がなくなり、様々な無線インフラを無線モジュールを差し替えるだけで安心して利用することが可能となる。

【0089】

次に認証の具体例について、携帯端末装置 1 a を例に以下説明する。

【0090】

無線モジュール 4 a、5 a、6 a を販売店で購入すると、それぞれ専用のキーモジュール 4 b、5 b、6 b が添付される。それぞれのモジュールには、認証に使うデータとして図 2 2 に示すようなデータが内部のメモリ 3 5、4 4 に記憶されている。認証用データは、モジュール ID、認証コード KEY_{ID}、暗号関数 $f_{ID}(x)$ 、その逆暗号関数 $f_{ID}^{-1}(x)$ から成り、無線モジュールとそのキーモジュールとは同じユニークなモジュール ID、認証コード KEY_{ID} が共に記憶され、逆暗号関数 $f_{ID}^{-1}(x)$ は無線モジュール側に、その暗号関数 $f_{ID}(x)$ はキーモジュール側に記憶される。認証コード KEY_{ID}、暗号関数 $f_{ID}(x)$ 、逆暗号関数 $f_{ID}^{-1}(x)$ も、無線モジュールとキーモジュールの組毎にユニークなものとなっている。

【0091】

最初に、キーモジュールに記憶された認証用データを携帯端末装置 1 a に登録する。携帯端末装置 1 a のキーパッド 1 0 1 の操作でキーモジュール登録処理を起動すると、制御部 1 0 4 は図 2 3 に示す処理を開始する。まず、スロット 2 a にキーモジュールを挿入する促進メッセージを表示器 1 0 2 に表示する (S 1 0 1)。ユーザが例えば PHS システム用のキーモジュール 4 b をスロット 2 a に挿入すると、携帯端末装置 1 a に内蔵の電源 1 0 8 からスロット 2 a を通じてキーモジュール 4 b に電力が供給されて各部が動作可能となる。制御部 1 0 4 はインタフェース 1 0 7、ソケット 1 0 9、コネクタ 4 1、インタフェース 4 2 および制御部 4 3 を通じてメモリ 4 4 に記憶されたモジュール ID 1、認証コード KEY_{ID1}、暗号関数 $f_{ID1}(x)$ を読み込み (S 1 0 2)、認証テーブルに保存する (S 1 0 3)。

【0092】

次に制御部 1 0 4 は他に登録するキーモジュールがあるか否かを表示器 1 0 2 にメッセージを表示してユーザに問い合わせ、他のキーモジュールがある場合 (S 1 0 4 で NO)、ステップ S 1 0 1 に戻って上述した処理を繰り返す。ユーザ

が P H S システム用以外に P D C システム用や C D M A システム用のモジュールを持っている場合、それらのキーモジュールをスロット 2 a に挿入することで、認証用データを携帯端末装置 1 a に登録する。登録するキーモジュールが他になければ (S 1 0 4 で Y E S) 、制御部 1 0 4 は処理を終了する。

【 0 0 9 3 】

図 2 4 に携帯端末装置 1 a のメモリ 1 0 6 上に設けられた認証テーブル 2 0 1 の内容例を示す。この例では、P H S 用の認証データ 2 0 2 、P D C 用の認証データ 2 0 3 、C D M A 用の認証データ 2 0 4 の 3 種類が設定されている。なお、エントリ 2 0 5 ~ 2 0 7 は実際の認証時に乱数が格納される部分であり、キーモジュールの登録時は N U L L になっている。

【 0 0 9 4 】

次に、無線モジュールを使用して携帯端末装置 1 a から移動体通信サービスを利用する際の認証処理について説明する。

【 0 0 9 5 】

携帯端末装置 1 a のキーパッド 1 0 1 の操作で無線モジュール登録処理を起動すると、制御部 1 0 4 は図 2 5 に示す処理を開始する。まず、スロット 2 a に無線モジュールを挿入する促進メッセージを表示器 1 0 2 に表示する (S 1 1 1) 。ユーザが例えば P H S システム用の無線モジュール 4 a をスロット 2 a に挿入すると、携帯端末装置 1 a に内蔵の電源 1 0 8 からスロット 2 a を通じて無線モジュール 4 a に電力が供給されて各部が動作可能となる。制御部 1 0 4 は、無線モジュール 4 a からモジュール I D が送られてくるのを待つ。

【 0 0 9 6 】

無線モジュール 4 a の制御部 3 4 は、電源が投入されると図 2 6 に示す認証処理を開始する。まず、メモリ 3 5 に記憶されたモジュール I D 1 を読み取って、インタフェイス 3 3 、コネクタ 3 1 を介して携帯端末装置 1 a に送出する (S 1 3 1) 。そして、携帯端末装置 1 a から応答データが送られてくるのを待つ。

【 0 0 9 7 】

携帯端末装置 1 a の制御部 1 0 4 は、このモジュール I D 1 をソケット 1 0 9 、インタフェイス 1 0 7 を通じて受け取ると (S 1 1 2) 、モジュール I D 1 で

図 2 4 の認証テーブル 2 0 1 を検索し、同じモジュール I D 1 が登録されているか否かを調べる (S 1 1 3)。同じモジュール I D 1 が登録されていない場合 (S 1 1 3 で N O)、認証失敗となる (S 1 1 4)。認証が失敗すると、制御部 1 0 4 は当該無線モジュール 4 a を不正なモジュールと判断し、当該無線モジュール 4 a を使用した制御を行わない。他方、同じモジュール I D 1 が登録されていた場合 (S 1 1 3 で Y E S)、それと組になって登録されている認証コード K E Y_{ID1}、暗号関数 $f_{ID1}(x)$ を認証テーブル 2 0 1 から読み取り (S 1 1 5)、乱数発生プログラム等によって乱数 R a n d を生成し (S 1 1 6)、K E Y_{ID1} と乱数 R a n d を連結したデータを暗号関数 $f_{ID1}(x)$ で暗号化し (S 1 1 7)、無線モジュール 4 a に暗号化データを送出する (S 1 1 8)。そして、無線モジュール 4 a から応答データが送られてくるのを待つ。なお、発生した乱数 R a n d は、後の処理のために認証テーブルに記憶しておく。

【0098】

無線モジュール 4 a の制御部 3 4 は、暗号化データを携帯端末装置 1 a から受け取ると (S 1 3 2)、その暗号化データを逆暗号関数 $f_{ID1}^{-1}(x)$ で復号し、認証コード K E Y_{ID1} と乱数 R a n d を得る (S 1 3 3)。そして、復号化して得た認証コード K E Y_{ID1} がメモリ 3 5 に記憶されている認証コード K E Y_{ID1} と一致するか否かを調べ (S 1 3 4)、一致しなければ異常コードを携帯端末装置 1 a に送出し (S 1 3 5)、処理を終了する。他方、一致すれば、前記復号化して得た乱数 R a n d を逆暗号関数 $f_{ID1}^{-1}(x)$ で暗号化し (S 1 3 6)、携帯端末装置 1 a に送出して (S 1 3 7)、処理を終了する。

【0099】

携帯端末装置 1 a の制御部 1 0 4 は、無線モジュール 4 a からの応答データを受け取ると (S 1 1 9)、それが異常コードであった場合 (S 1 2 0)、認証失敗とする (S 1 1 4)。応答内容が異常コードでない場合、応答内容を暗号関数 $f_{ID1}(x)$ で復号し、乱数 R a n d を得る (S 1 2 1)。そして、この復号化した得た乱数 R a n d とステップ S 1 1 6 で自ら生成した乱数 R a n d とが一致するか否かを調べ (S 1 2 2)、一致しない場合、認証失敗とする (S 1 1 4)。一致した場合は認証成功となる (S 1 2 3)。以後、制御部 1 0 4 は、当該無

線モジュール 4 a を使った P H S システムの利用を可能とする。認証成功の場合、制御部 1 0 4 は、携帯端末装置 1 a が若しロック状態であればそれを解除し（S 1 2 4）、所定の監視処理を起動し（S 1 2 5）、図 2 5 の処理を終了する。ステップ S 1 2 4、S 1 2 5 の詳細については後述する。

【0 1 0 0】

以上は P H S システムの無線モジュール 4 a を使う場合の携帯端末装置 1 a と無線モジュール間の相互認証について説明したが、P D C システムの無線モジュール 5 a、C D M A システムの無線モジュール 6 a を使用する場合にも、携帯端末装置 1 a と無線モジュール間で同様な相互認証が行われ、認証成功時にのみ当該無線モジュール 5 a、6 a の利用が可能となる。また、携帯端末装置 1 a を例にしてキーモジュールの登録と無線モジュール使用時の認証処理を説明したが、図 2 3 および図 2 5 に示されるような機能は P D A 1 b および P C 1 c の M P U 1 1 1 によっても提供されているため、携帯端末装置 1 a と同じ作業を実施することにより、P D A 1 b および P C 1 c でも無線モジュール 4 a、5 a、6 a を使用した移動体通信サービスの利用が可能である。

【0 1 0 1】

次に、図 2 5 のステップ S 1 2 4、S 1 2 5 について、携帯端末装置 1 a の場合を例に説明する。P D A 1 b、P C 1 a の場合も同様である。

【0 1 0 2】

ステップ S 1 2 5 で起動される監視処理の一例を図 2 7 に示す。この監視処理は携帯端末装置 1 a の電源スイッチのオン、オフにかかわらず実行される。監視処理が起動されると、制御部 1 0 4 はスロット 2 a から通信装置（無線モジュール）が外されたかどうか、キーパッド 1 0 1 から所定のキー操作によって監視停止が指示されたかどうかを監視する（S 1 4 1、S 1 4 2）。スロット 2 a から通信装置が外されたかどうかは、例えばソケット 1 0 9 の所定の端子がコネクタ 3 1 に接続されているときの電氣的な状態を示すか否かや、通信装置の制御部と交信を試みる等の任意の方法が利用できる。

【0 1 0 3】

スロット 2 a から通信装置が外された場合（S 1 4 1 で Y E S）、制御部 1 0

4 は、携帯端末装置 1 a に対するユーザの一切の入力を無効とするロック状態とする（S 143）。従って、キーパッド 101 による操作は一切行えず、メモリ 106 に記憶された電話帳などの情報を表示器 102 に表示させることもできなくなる。PAD 1 b のようにタブレット 121 を有する装置ではペン入力も無効となり、マウスを有する場合にはマウス入力も無効となる。その後、制御部 104 は、スロット 2 a に通信装置（無線モジュール）が挿入されたか否かを監視し（S 144）、挿入されたら、図 25 に示した相互認証処理におけるステップ S 112 へと進む。この結果、外された通信装置が再びスロット 2 a に挿入されると図 25 に示した相互認証処理が実施される。そして、認証が成功すると、ステップ S 124 において携帯端末装置 1 a のロック状態が解除される。これによって、ユーザによる入力操作が可能となる。

【0104】

他方、監視処理中に監視停止の指示があった場合（S 142 で YES）、制御部 104 は図 27 の監視処理を終了する。この後、スロット 2 a から通信装置を外しても装置はロック状態にならない。これは、携帯端末装置 1 a に対する新たなキーモジュールの登録作業や前述したワイヤレス接続用の通信装置の登録作業などを可能にするためである。

【0105】

図 28 は移動体通信サービスを利用する際に使用する通信装置の別のセットの例を示し、7 a はお父さん用の無線モジュール、7 b はそのキーモジュール、8 a はお母さん用の無線モジュール、8 b はそのキーモジュール、9 a は自分用の無線モジュール、9 b はそのキーモジュールである。無線モジュール 7 a、8 a、9 a は、所定の移動体通信サービス用（例えば PHS システム用）のもので、端末装置のスロットに挿入して使用する。また、キーモジュール 7 a、8 a、9 a は、前述したキーモジュール 4 b、5 b、6 b と同じ目的のために使用するモジュールである。全てのモジュールは、前述したキーモジュール 4 b、5 b、6 b と同じ規格で統一された同一の外形形状を有する。更に、無線モジュール 7 a、8 a、9 a は、端末装置のスロットに挿入したときに装置外にはみ出る部分（図 28 でハッチングを施した部分）が、利用する個人に応じた色で色付けされて

おり、色を見れば、どの人の無線モジュールであるかが即座に認識できるようになっている。

【0106】

特定のプロバイダーに、申請者各員毎の住所、氏名、パスワード等の所定の事項を記載した申込書を郵送ないしインターネット経由で送信すると、プロバイダーから各員用の無線モジュールとキーモジュールのセットが送られてくる。図28に示したモジュールのセットは、このようにして購入したもので、個々の無線モジュール7a、8a、9aのメモリ35には、当該プロバイダーに接続するために必要な一切の情報（プロバイダー接続情報と称す）が事前に記憶されている。プロバイダー接続情報には、プロバイダー側が各員に付与したユーザ名、各員が申請したパスワード、最寄りのアクセスポイントの電話番号等が含まれる。使用に際しては、前述と同様にキーモジュール7b、8b、9bに記憶された認証用データを例えば携帯端末装置1aに登録し、次いで、個人の無線モジュール7aまたは8aまたは9aを携帯端末装置1aのスロット2aに挿入し、認証を得た後、利用する。インターネットを利用する場合、無線モジュール7a、8a、9aに記憶されたプロバイダー接続情報が利用される。

【0107】

図29に携帯端末装置1aのスロット2aに例えば無線モジュール7aを挿入して、インターネットに接続する際の処理の一例を示す。ユーザが携帯端末装置1aのキーパッド101の操作で制御部104が有するブラウザ機能を起動すると、ブラウザが立ち上がる（S151）。次に制御部104は、スロット2aに挿入された無線モジュール7aのメモリ35からプロバイダー接続情報を読み出し、メモリ106に記憶する（S152）。次に、パスワードの入力を促すメッセージを表示器102に表示してユーザからパスワードを入力させ（S153）、メモリ106に記憶したプロバイダー接続情報中のパスワードと比較する（S154）。パスワードが不一致のときはエラー処理を行い、一致した場合は、メモリ106に記憶したプロバイダー接続情報中の電話番号を用いて無線モジュール7aからアクセスポイントに発呼し、ユーザIDおよびパスワードを送ってプロバイダーに接続する（S155）。以後、ユーザが指定するURLに従ってイ

ンターネット上のホームページをアクセスする。

【0 1 0 8】

以上は無線モジュール 7 a を用いたが、他の無線モジュール 8 a、9 a に差し替えれば他の個人もインターネットを即利用することができる。また、携帯端末装置 1 a だけでなく、PDA 1 b や PC 1 c のスロットに挿入することで、これらからもインターネットに接続することができる。

【0 1 0 9】

なお、以上の説明では、ユーザからのブラウザ起動の指示を待ってプロバイダーに接続したが、図 2 9 の処理を図 2 5 のステップ S 1 2 5 の直後に自動的に実行することにより、無線モジュール 7 a、8 a、9 a を端末装置のスロットに挿入すれば、プロバイダーに即接続される構成にすることができる。

【0 1 1 0】

【発明の効果】

以上説明したように本発明によれば、以下のような効果が得られる。

【0 1 1 1】

色分けされた様々な通信装置を差し替えることで様々な無線インフラに対応でき、且つ現在どのような通信装置を使用しているかを端末装置のスロットに通信装置が挿入された状態で外部から極めて容易に確認することができる。

【0 1 1 2】

通信装置と同形状のキーモジュールによって認証用のデータを端末装置に一旦登録しておけば、通信装置を挿入する都度、パスワードなどをユーザが一々入力しなくても通信装置と端末装置間で認証処理が自動的に行われるため、他人による通信装置の悪用を防止するために必要なユーザの作業量を削減することができる。また、登録には必ずキーモジュールが必要であるため、パスワード入力より安全性が高い。

【0 1 1 3】

端末装置と通信装置との間で認証が成立した後、通信装置がスロットから取り出されたとき、端末装置を利用者からの入力を一切受け付けないロック状態とする構成にあっては、通信装置に鍵（キー）の機能を持たせることができる。

【0114】

特定のプロバイダーに接続するのに必要な情報を記憶するメモリを備えた通信装置によれば、通信装置を購入すれば直ちにインターネットのプロバイダーへの接続が可能になり、インターネットを手軽に利用できる通信装置を提供できる。

【0115】

端末間をワイヤレス接続する通信装置をその伝送速度に応じて色分けした構成にあっては、現在どのような伝送速度の通信装置を使用しているかを端末装置のスロットに通信装置が挿入された状態で外部から極めて容易に確認することができる。

【0116】

本発明の通信装置セット及び端末間ワイヤレス接続方法によれば、同じセットの通信装置を端末装置のスロットに挿入するといった簡単な作業を行うだけで、通信アドレスやデータ暗号化用の鍵などの設定が行え、複数の端末間を手軽にワイヤレス接続することができる。

【図面の簡単な説明】

【図1】

本発明の一実施の形態を示すシステム構成図である。

【図2】

ワイヤレス接続用の通信装置の構成例を示すブロック図である。

【図3】

携帯端末装置の構成例を示すブロック図である。

【図4】

PDAの構成例を示すブロック図である。

【図5】

ユーザが購入した1セット分の通信装置の外観の概略と記憶情報の一例を示す図である。

【図6】

端末装置へのワイヤレス接続用通信装置の登録処理の第1の例を示すフローチ

ャートである。

【図 7】

ワイヤレス接続用通信装置の登録処理によって生成される自通信装置情報テーブル、送信先一覧テーブル、送信先選択画面の例を示す図である。

【図 8】

ワイヤレス接続用通信装置間で授受される送信データのフォーマット例を示す図である。

【図 9】

ユーザが購入した 1 セット分の通信装置の外観の概略と記憶情報の他の例を示す図である。

【図 1 0】

ユーザが購入した 1 セット分の通信装置の外観の概略と記憶情報の更に別の例を示す図である。

【図 1 1】

端末装置へのワイヤレス接続用通信装置の登録処理の第 2 の例を示すフローチャートである。

【図 1 2】

ワイヤレス接続用通信装置の登録処理によって生成される自通信装置情報テーブル、送信先一覧テーブル、送信先選択画面の他の例を示す図である。

【図 1 3】

端末装置へのワイヤレス接続用通信装置の登録処理の第 3 の例を示すフローチャートである。

【図 1 4】

端末装置へのワイヤレス接続用通信装置の登録処理の第 4 の例を示すフローチャートである。

【図 1 5】

ワイヤレス接続する通信装置群の一例を示す図である。

【図 1 6】

端末装置へのワイヤレス接続用通信装置の登録処理の第 5 の例を示すフローチャートである。

ャートである。

【図 1 7】

中継装置を使って異なるセットの通信装置間で通信する構成例を示すブロック図である。

【図 1 8】

中継装置の各スロット毎に生成される自通信装置情報テーブル、送信先情報テーブルの例を示す図である。

【図 1 9】

移動体通信サービスを利用する際に使用する通信装置のセットの概略を示す図である。

【図 2 0】

移動体通信サービスを利用する際に使用する通信装置の構成例を示すブロック図である。

【図 2 1】

キーモジュールの構成例を示すブロック図である。

【図 2 2】

無線モジュールおよびキーモジュールに記憶されている認証用データの例を示す図である。

【図 2 3】

端末装置へのキーモジュールによる認証用データの登録処理の一例を示すフローチャートである。

【図 2 4】

端末装置のメモリ上に設けられた認証テーブルの内容例を示す図である。

【図 2 5】

端末装置側の認証処理の一例を示すフローチャートである。

【図 2 6】

無線モジュール側の認証処理の一例を示すフローチャートである。

【図 2 7】

端末装置側が認証成立時に起動する監視処理の一例を示すフローチャートであ

る。

【図 2 8】

移動体通信サービスを利用する際に使用する通信装置の別のセットの概略を示す図である。

【図 2 9】

端末装置から無線モジュールを使用してインターネットに接続する際の処理の一例を示すフローチャートである。

【符号の説明】

1 a … 携帯端末装置

1 b … P D A

1 c … P C

2 a ～ 2 c … スロット

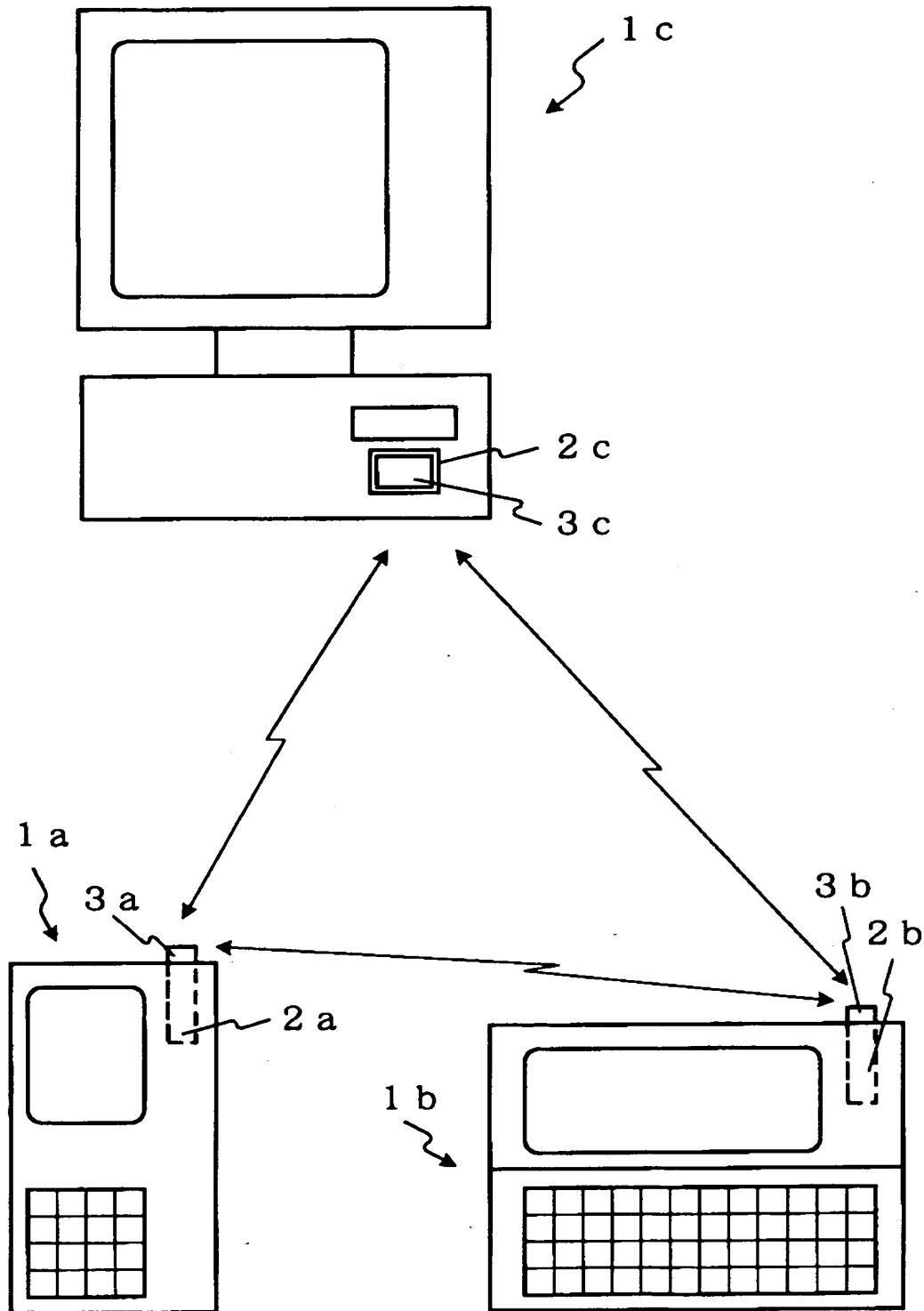
3 a ～ 3 c … ワイヤレス接続用の通信装置

4 a ～ 9 a … 移動体通信サービス接続用の無線モジュール（通信装置）

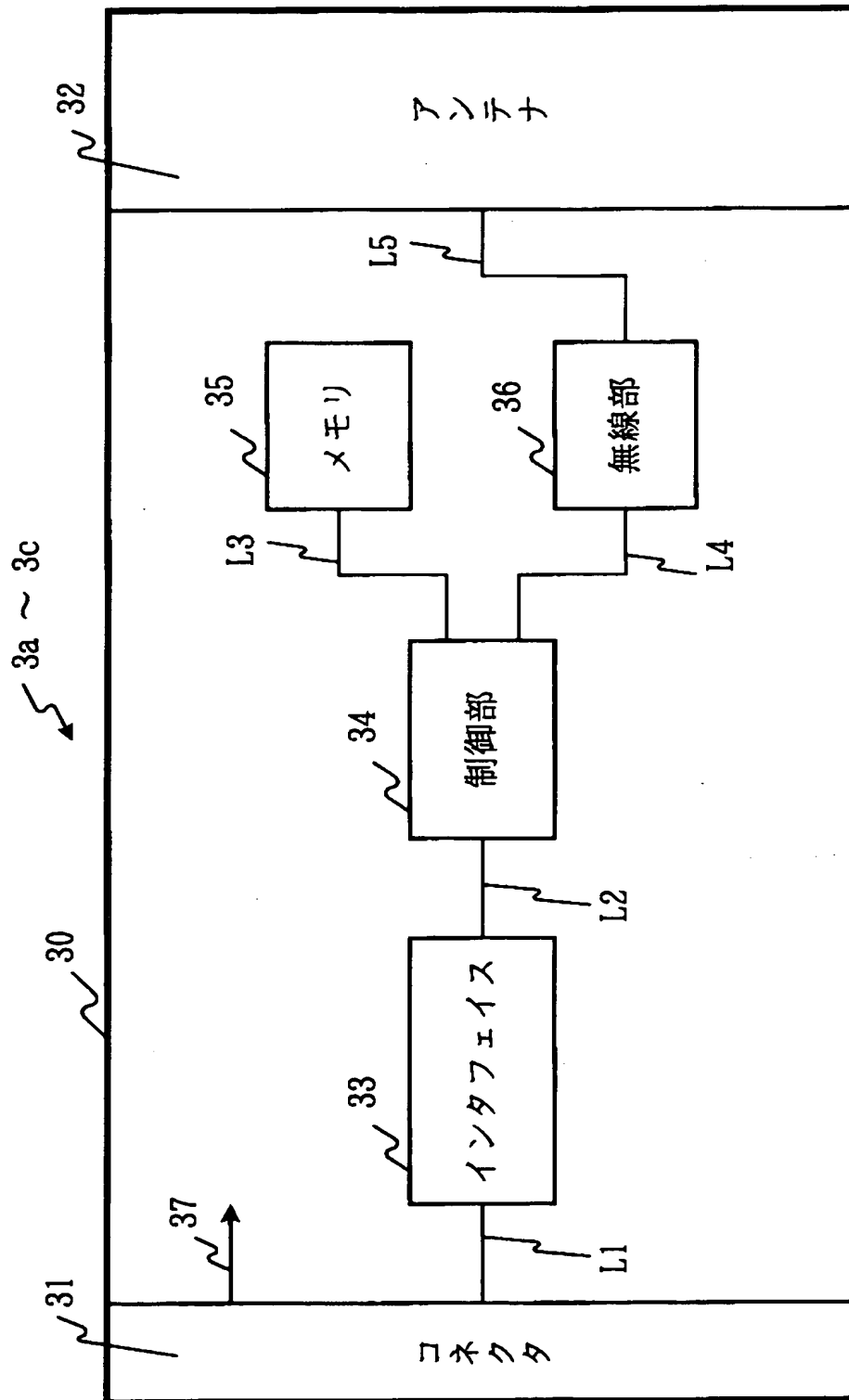
4 b ～ 9 b … キーモジュール

【書類名】 図面

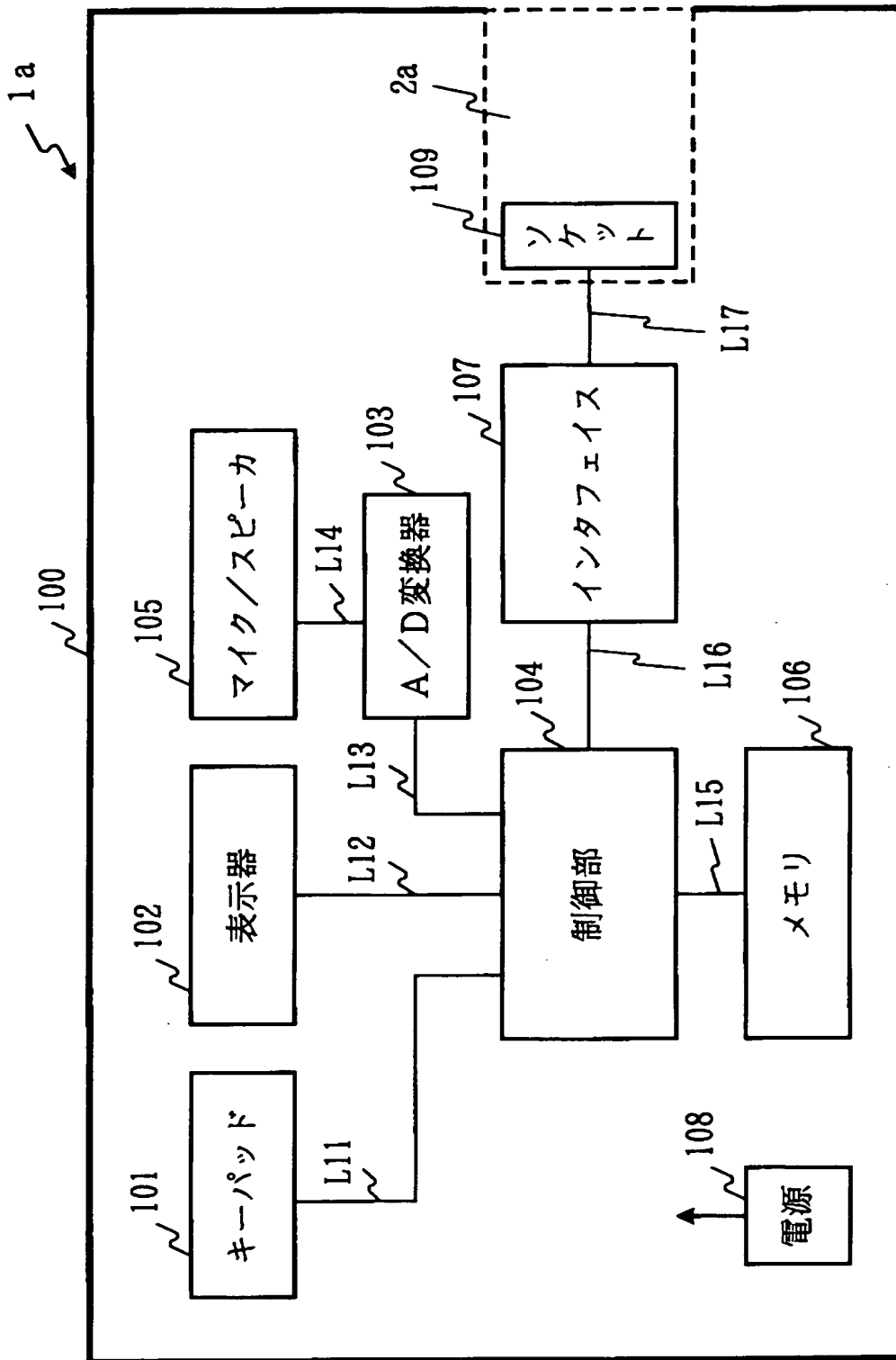
【図 1】



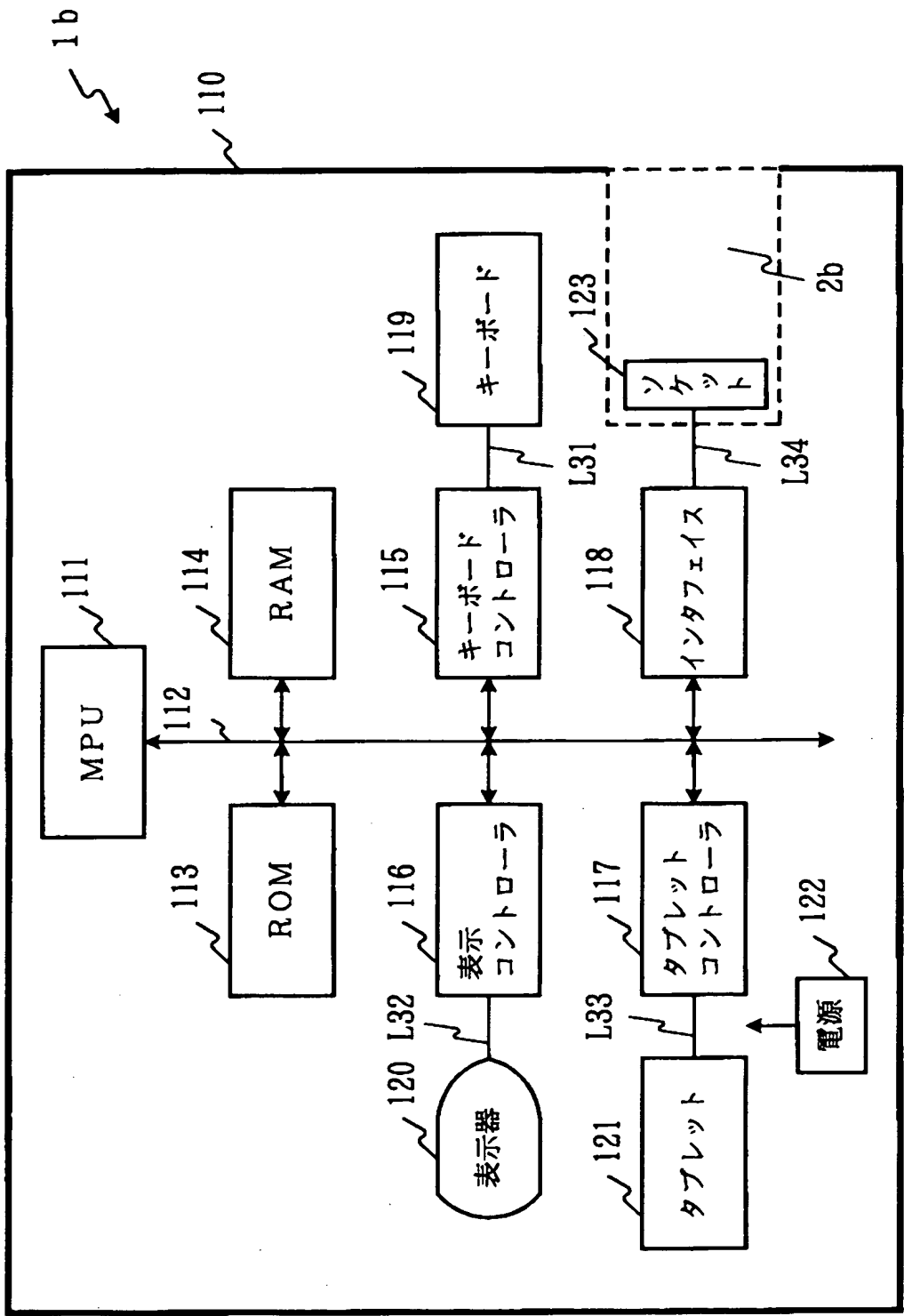
【図 2】



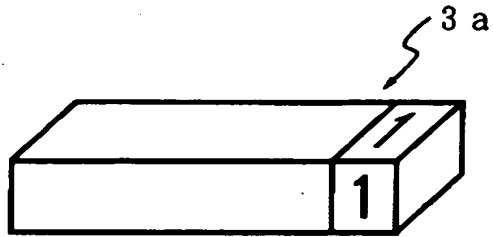
【図 3】



【図 4】



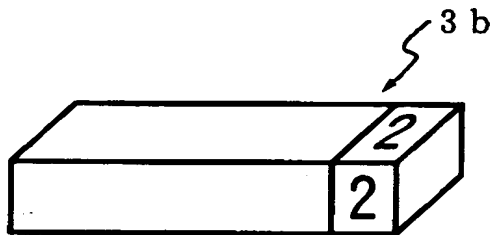
【図 5】



自通信装置 3 a の通信アドレス

他通信装置 3 b, 3 c の通信アドレス

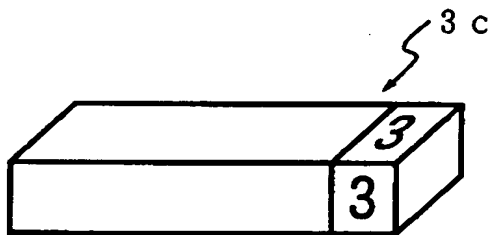
共通鍵 K



自通信装置 3 b の通信アドレス

他通信装置 3 a, 3 c の通信アドレス

共通鍵 K

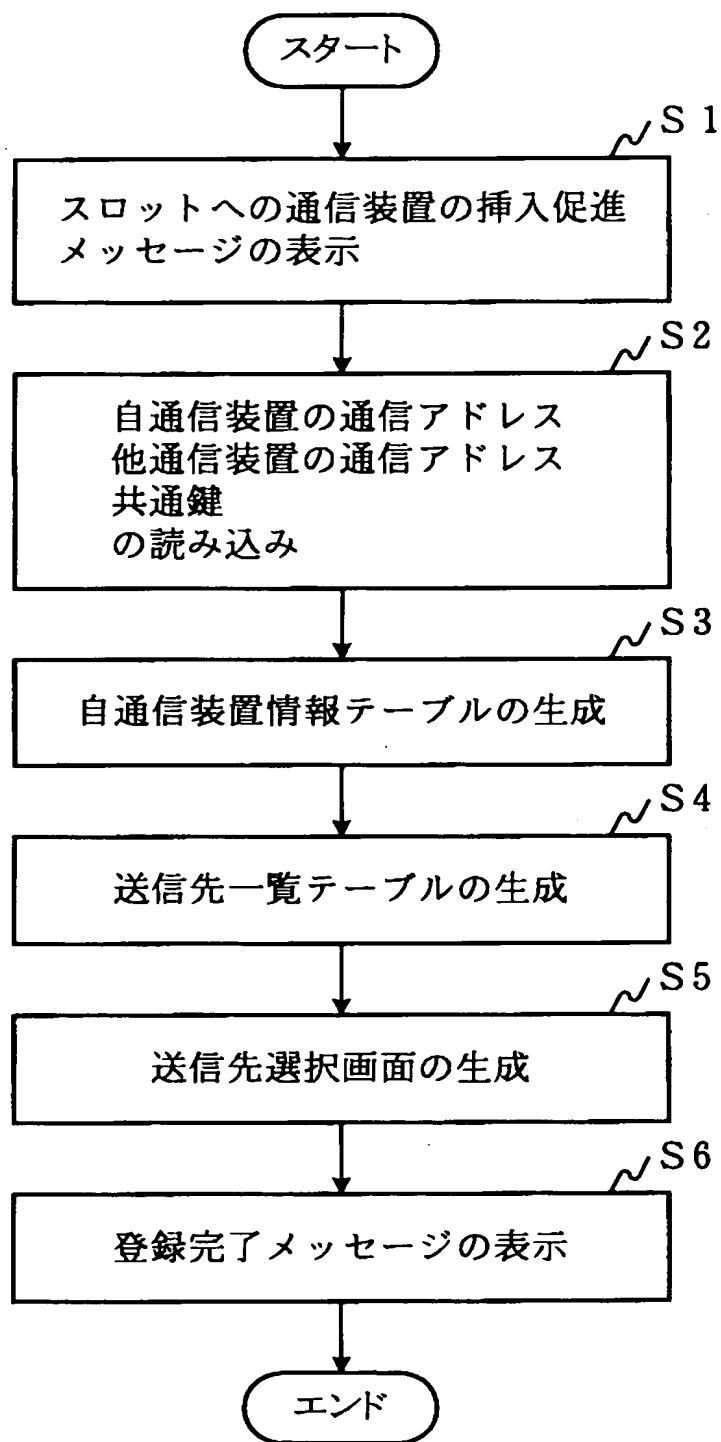


自通信装置 3 c の通信アドレス

他通信装置 3 a, 3 b の通信アドレス

共通鍵 K

【図 6】



【図 7】

1 3 0

(a)

通信装置番号	通信アドレス	鍵
1	通信装置 3 a の 通信アドレス	共通鍵 K

1 3 1

(b)

通信装置番号	通信アドレス	鍵
2	通信装置 3 b の 通信アドレス	共通鍵 K
3	通信装置 3 c の 通信アドレス	共通鍵 K

1 3 2

(c)

送信先は？

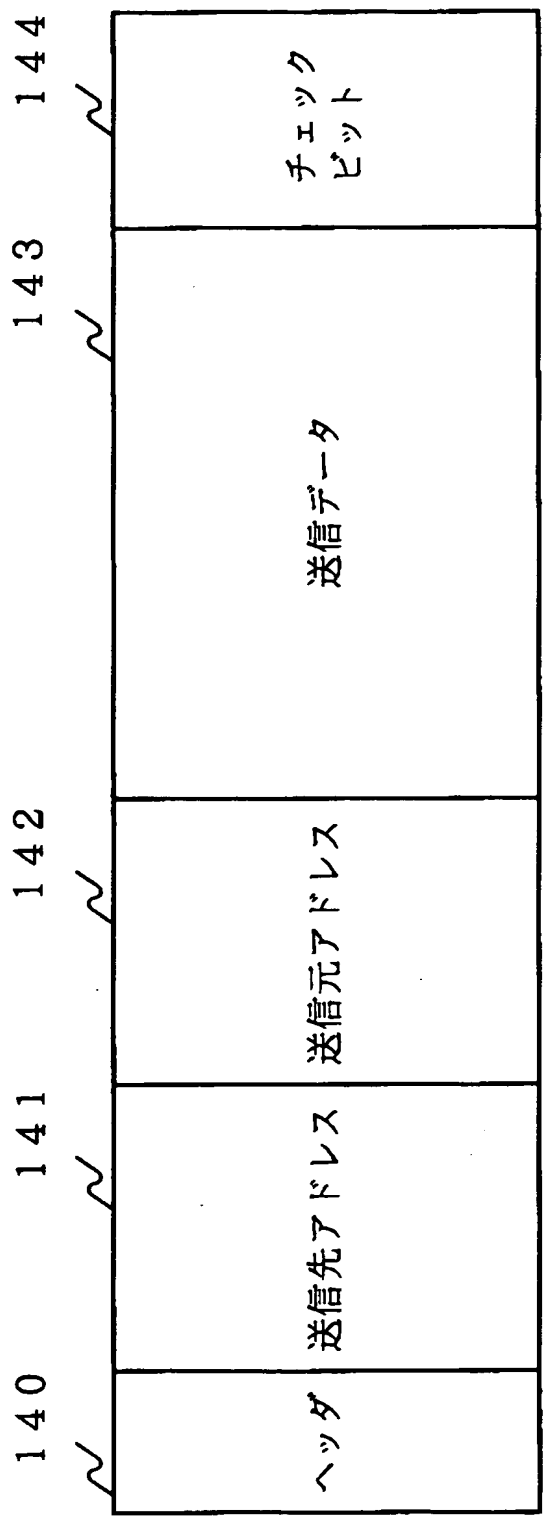
2

番

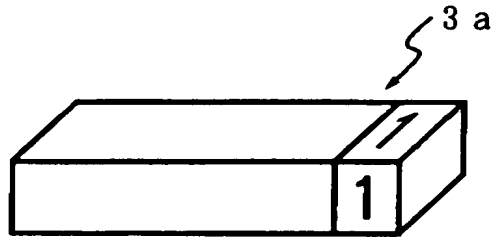
3

番

【図 8】



【図 9】

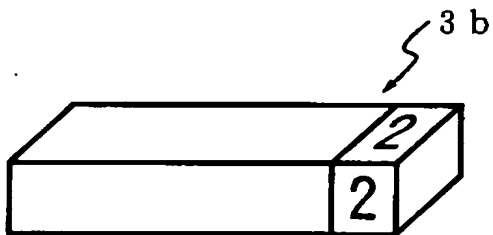


自通信装置 3 a の通信アドレス

他通信装置 3 b, 3 c の通信アドレス

自通信装置 3 a の秘密鍵

他通信装置 3 b, 3 c の公開鍵

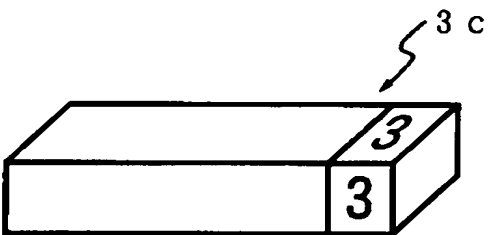


自通信装置 3 b の通信アドレス

他通信装置 3 a, 3 c の通信アドレス

自通信装置 3 b の秘密鍵

他通信装置 3 a, 3 c の公開鍵



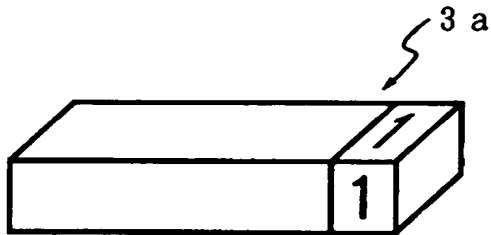
自通信装置 3 c の通信アドレス

他通信装置 3 a, 3 b の通信アドレス

自通信装置 3 c の秘密鍵

他通信装置 3 a, 3 b の公開鍵

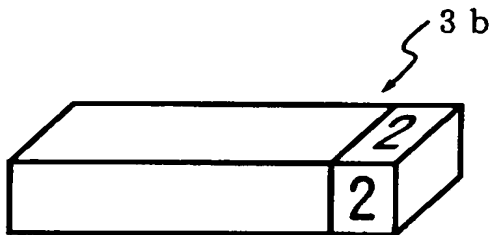
【図 1 0】



自通信装置 3 a の通信アドレス

自通信装置 3 a の秘密鍵

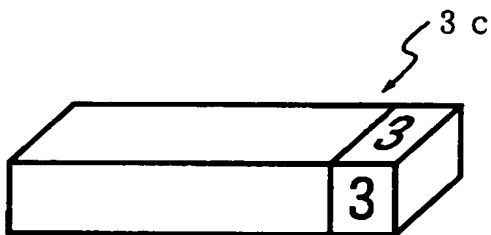
自通信装置 3 a の公開鍵



自通信装置 3 b の通信アドレス

自通信装置 3 b の秘密鍵

自通信装置 3 b の公開鍵

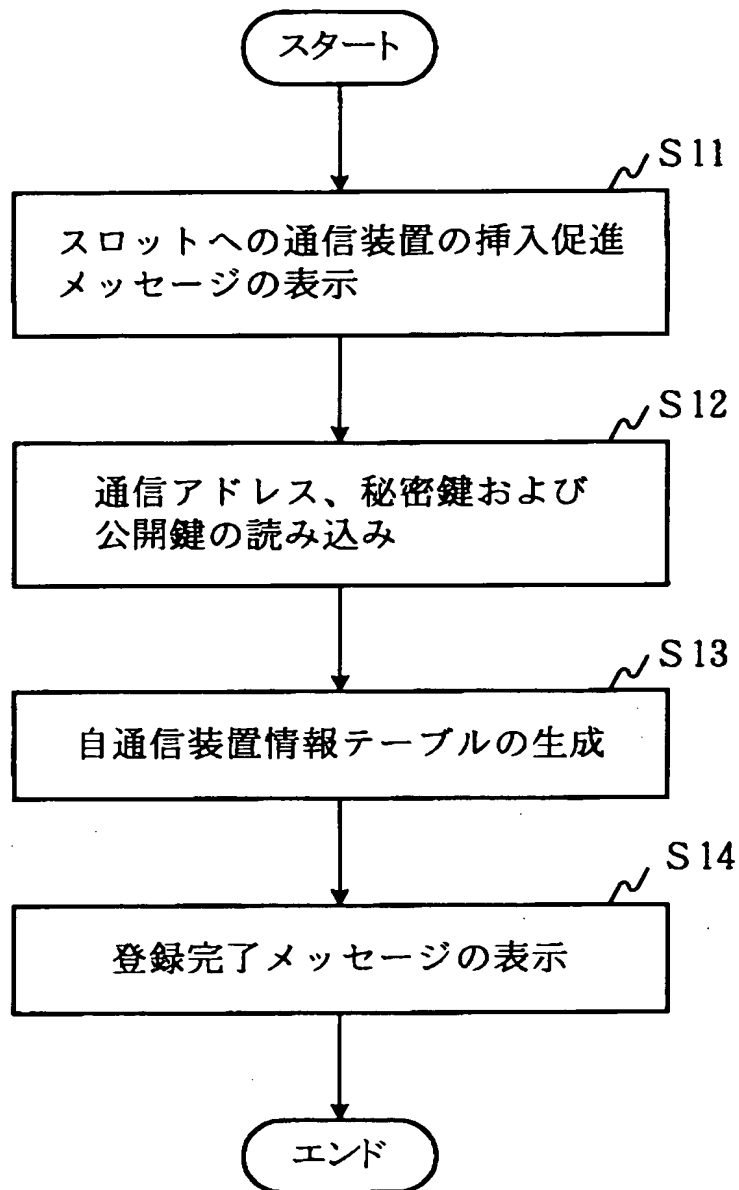


自通信装置 3 c の通信アドレス

自通信装置 3 c の秘密鍵

自通信装置 3 c の公開鍵

【図 1 1】



【図 1 2】

通信装置番号	通信アドレス	鍵	
1	通信装置 3 a の通信アドレス	通信装置 3 a の秘密鍵	通信装置 3 a の公開鍵

(a)

通信装置番号	通信アドレス	鍵	
2	通信装置 3 b の通信アドレス	通信装置 3 b の公開鍵	
3	通信装置 3 c の通信アドレス	通信装置 3 c の公開鍵	

(b)

送信先は？

2

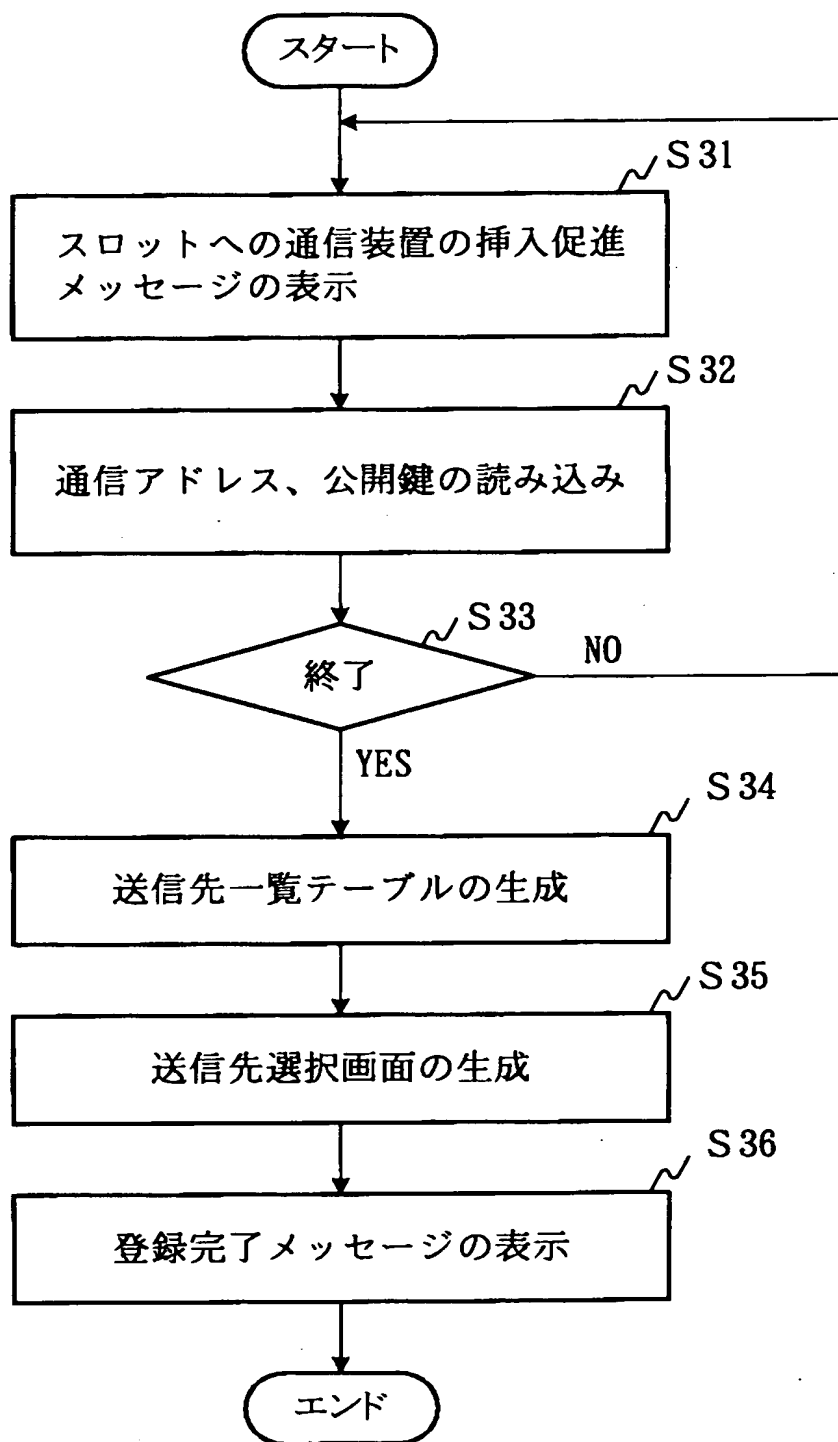
番

3

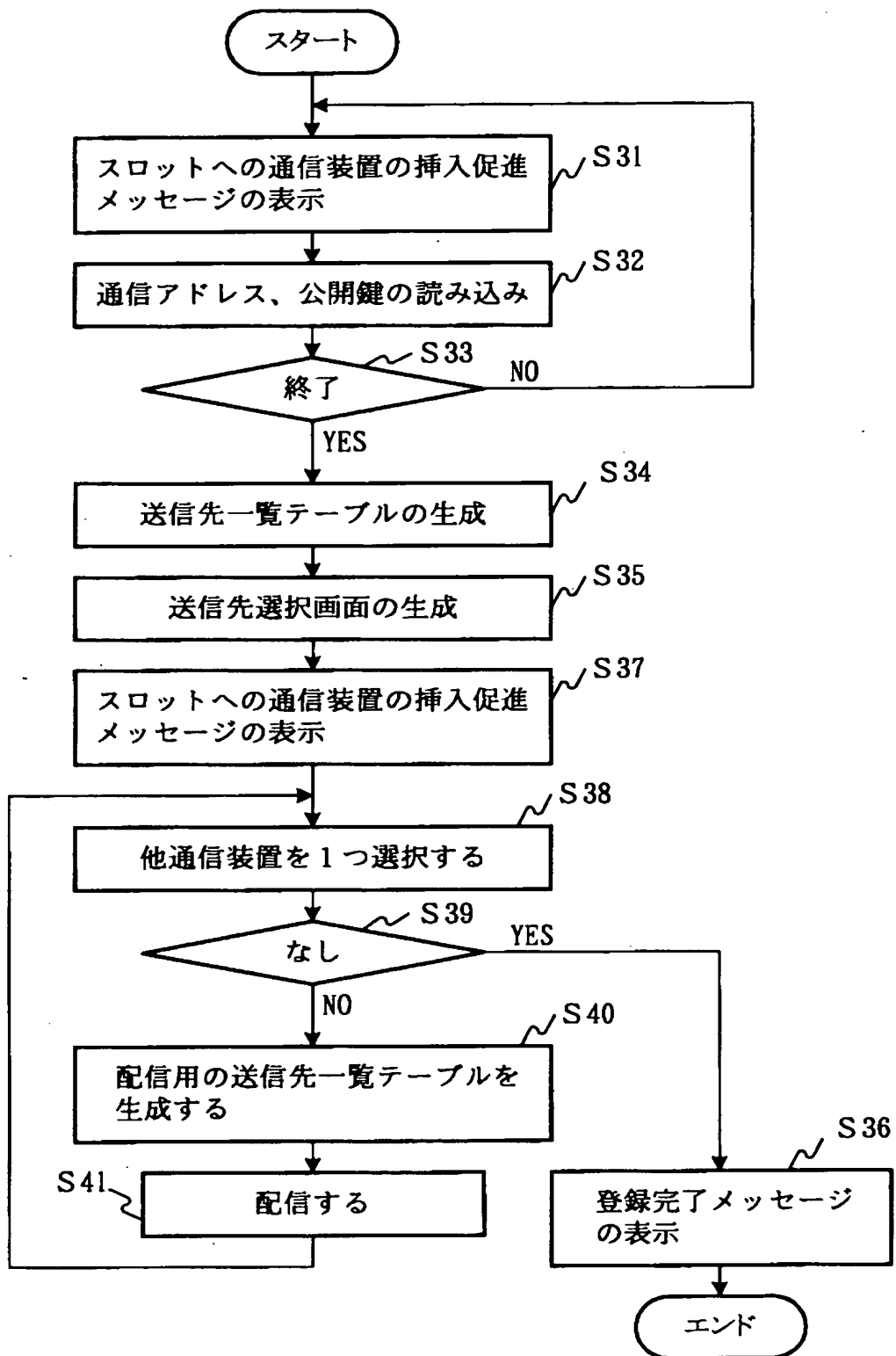
番

(c)

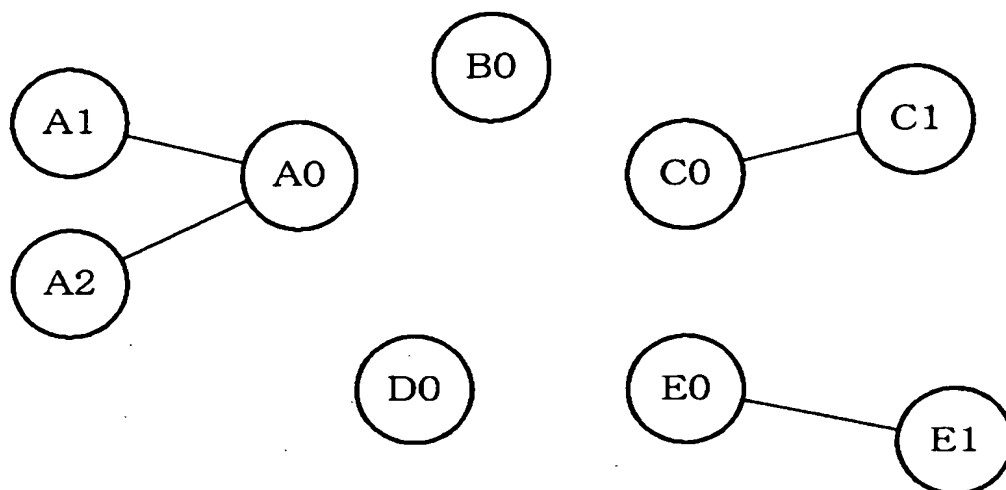
【図 1 3】



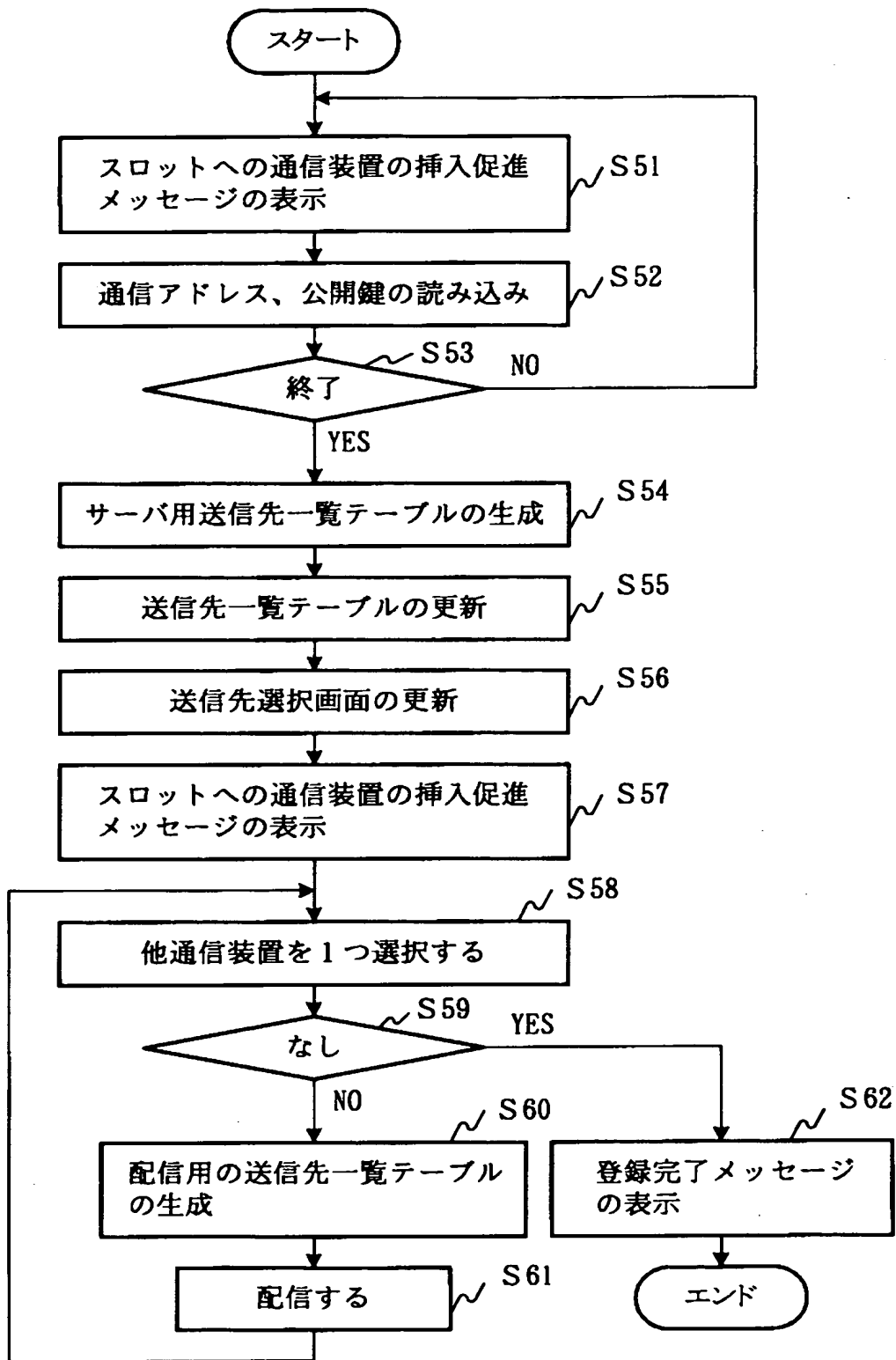
【図 1 4】



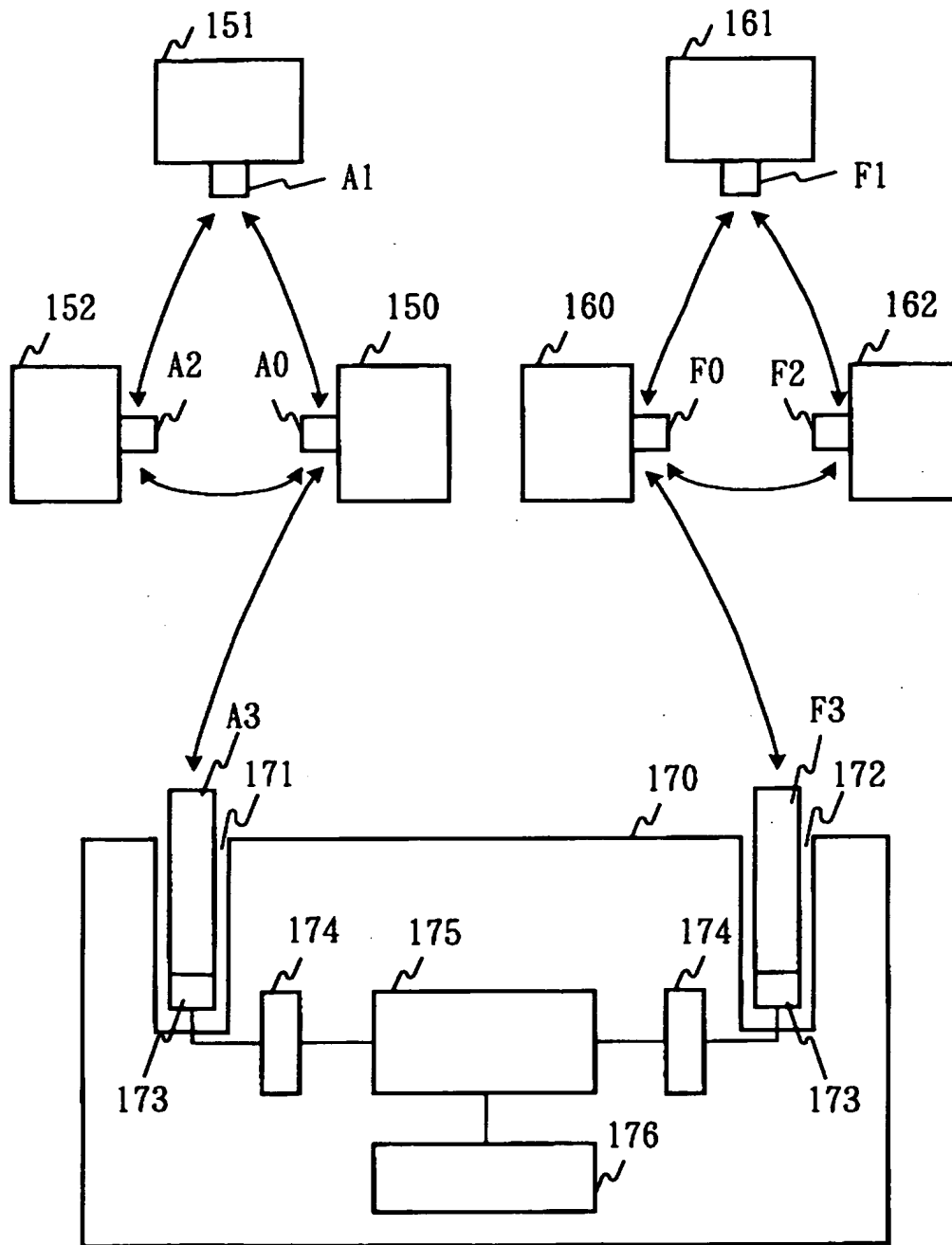
【図 1 5】



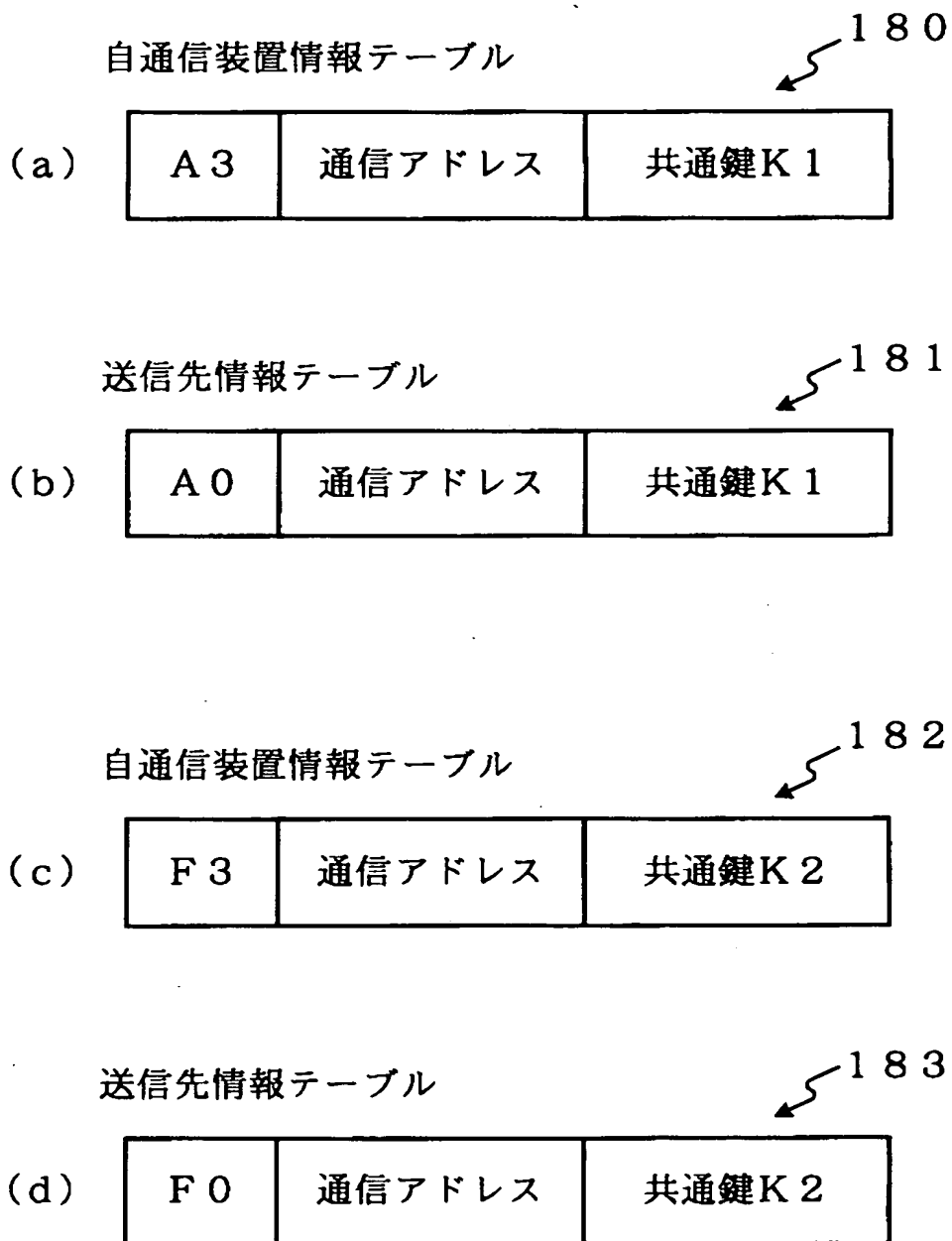
【図 1 6】



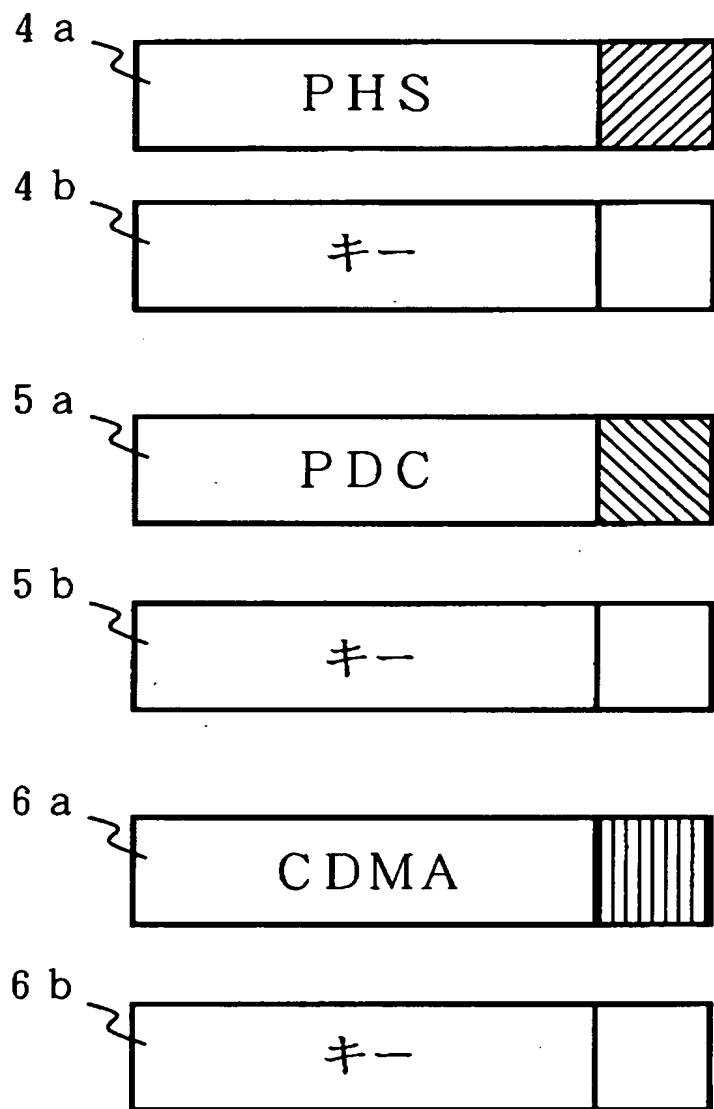
【図 1 7】



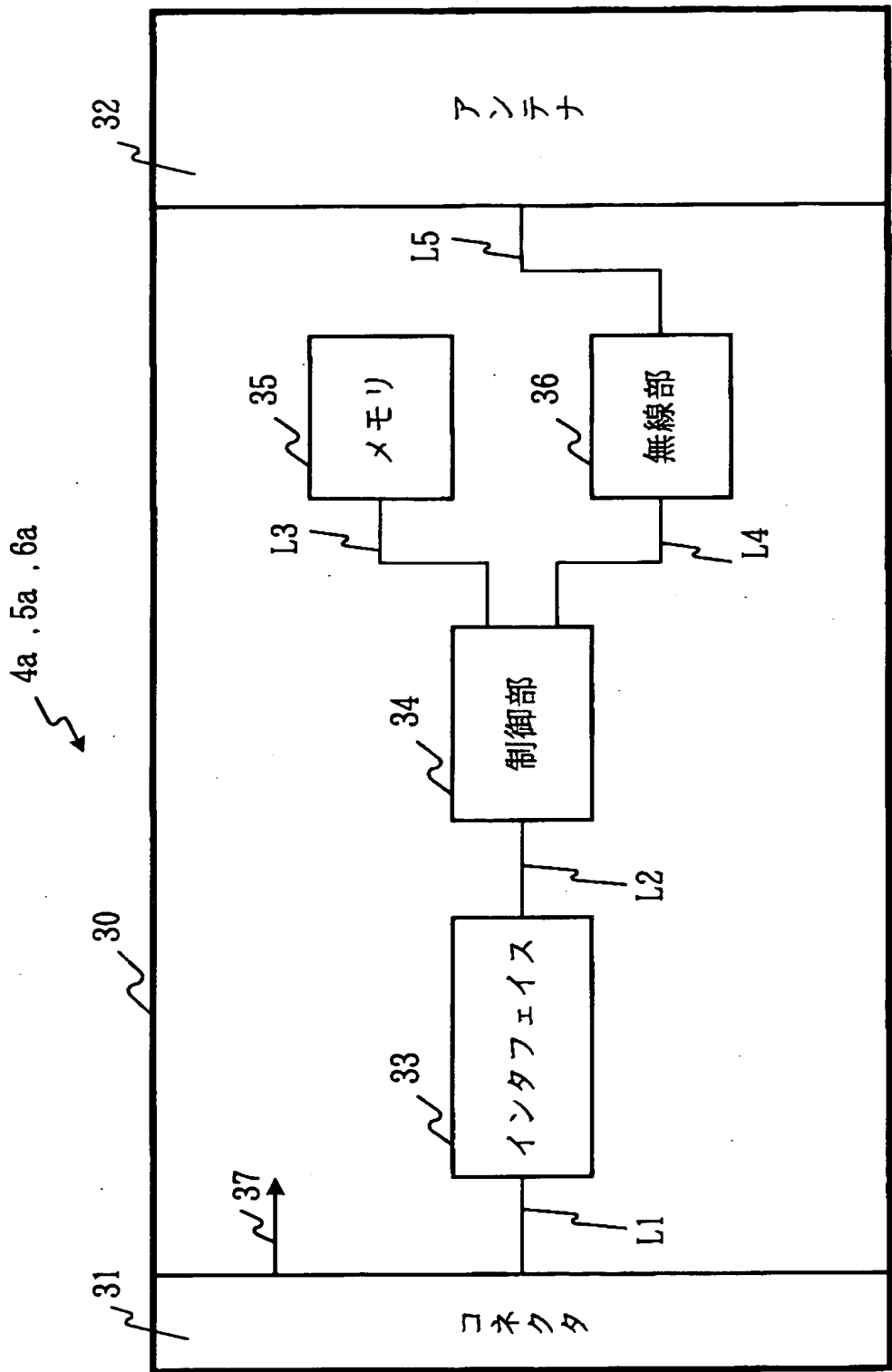
【図 1 8】



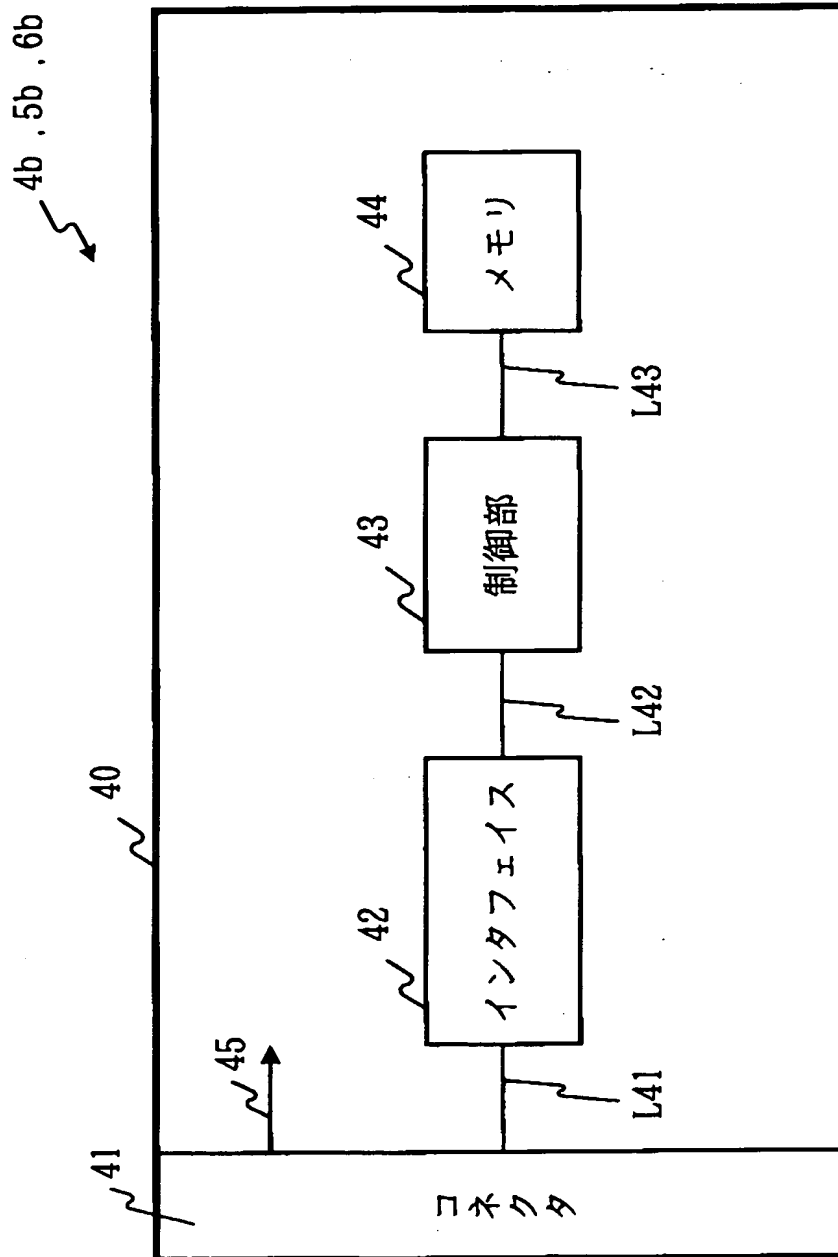
【図 1 9】



【図 2 0】



【図 2 1】



【図 2 2】

4 a

$ID1, KEY_{ID1}, f_{ID1}^{-1}(x)$

4 b

$ID1, KEY_{ID1}, f_{ID1}(x)$

5 a

$ID2, KEY_{ID2}, f_{ID2}^{-1}(x)$

5 b

$ID2, KEY_{ID2}, f_{ID2}(x)$

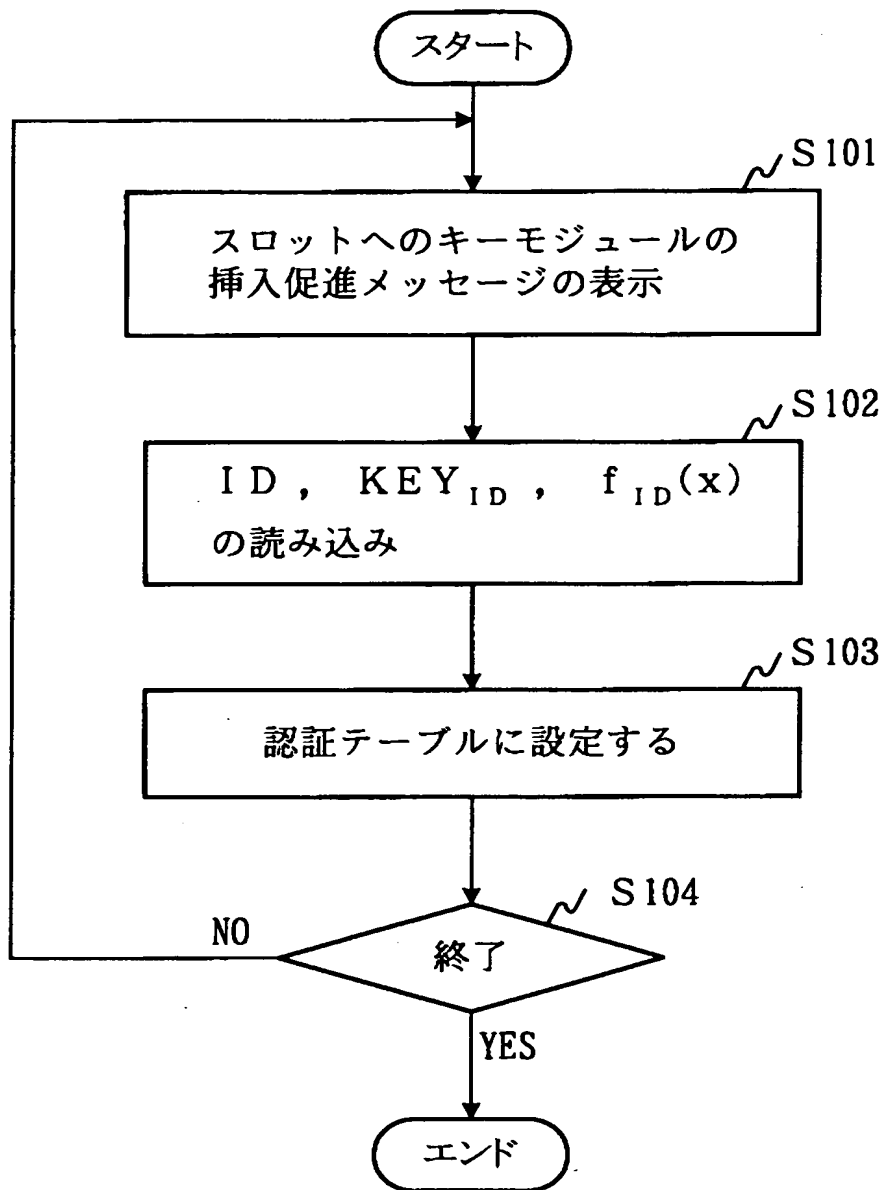
6 a

$ID3, KEY_{ID3}, f_{ID3}^{-1}(x)$

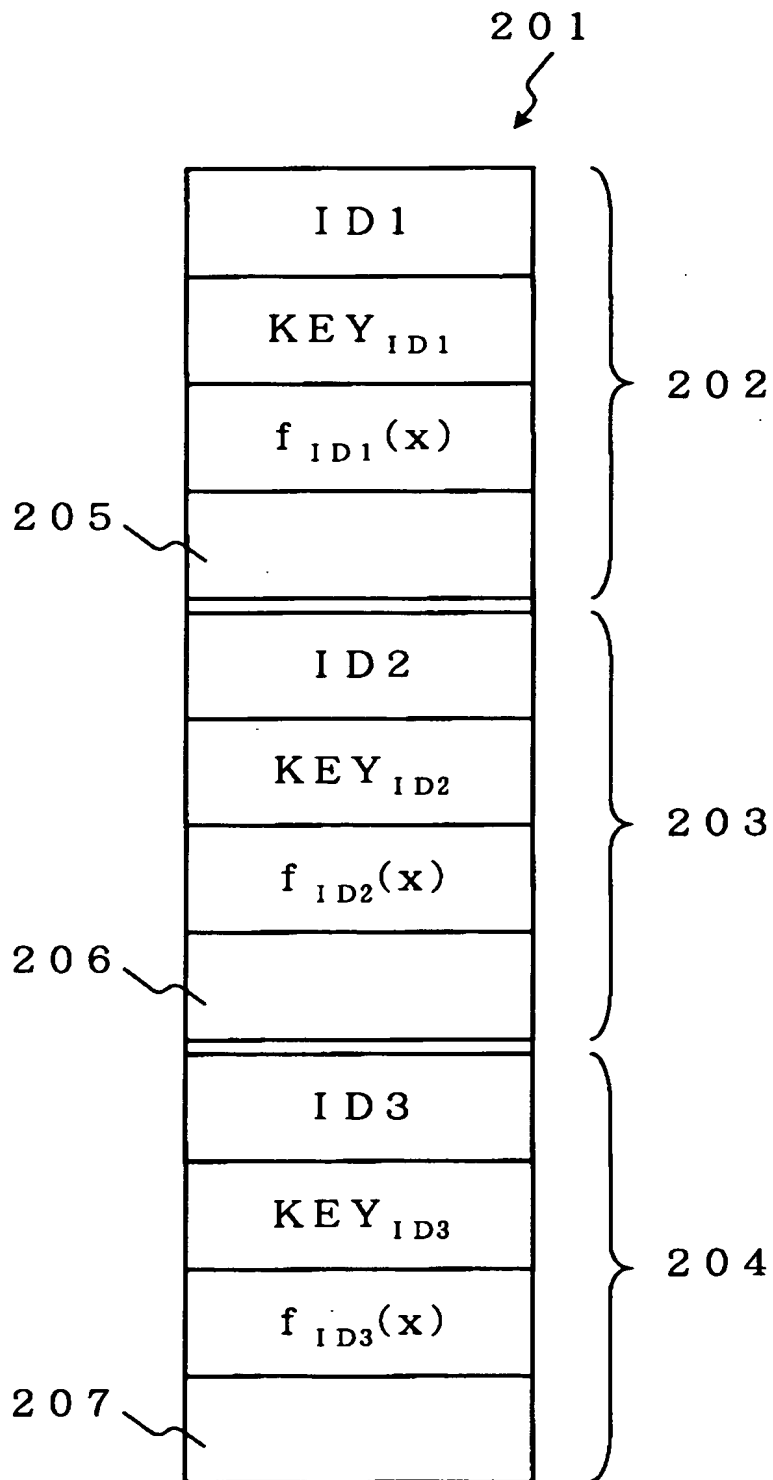
6 b

$ID3, KEY_{ID3}, f_{ID3}(x)$

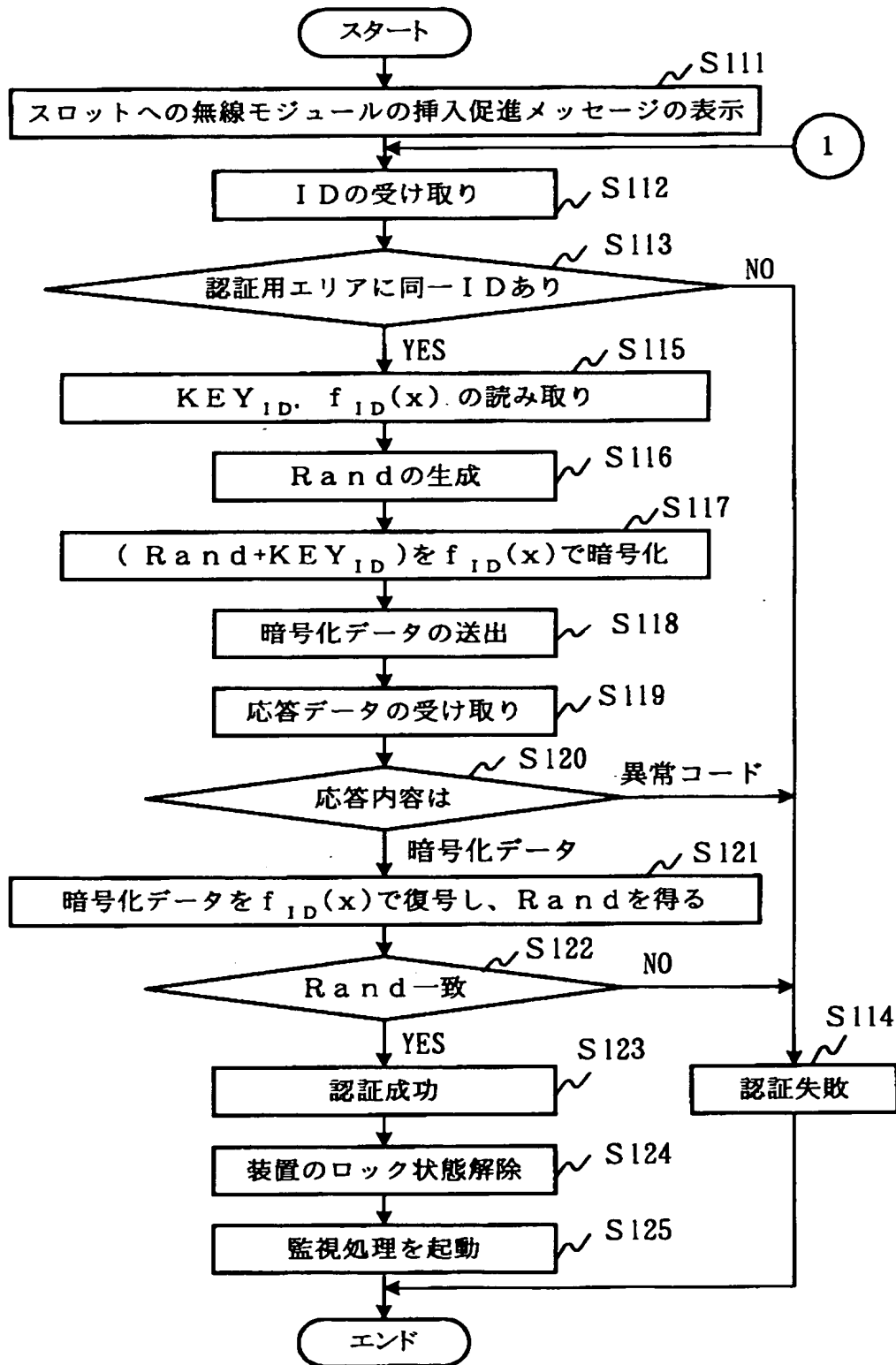
【図 2 3】



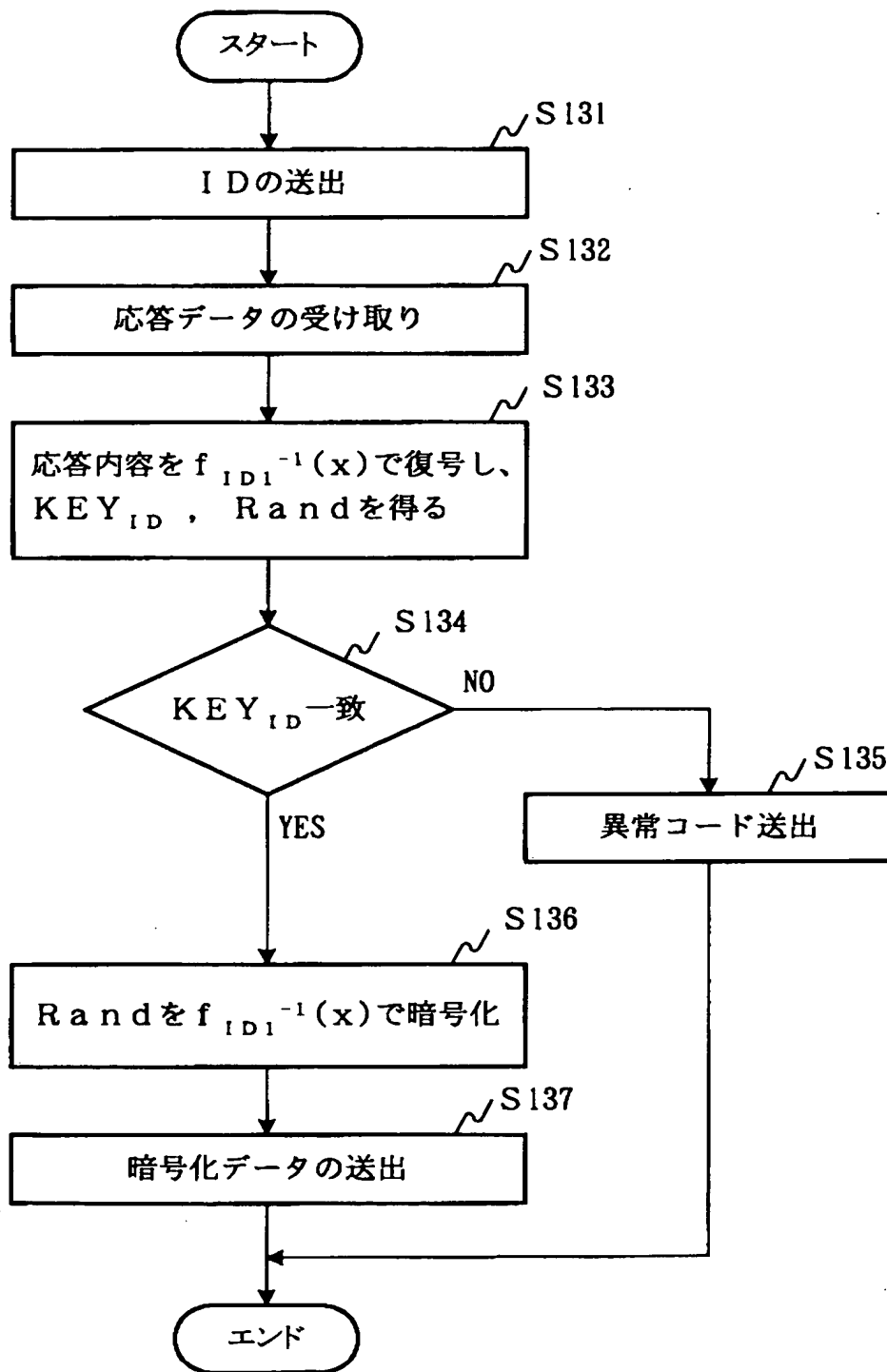
【図 2 4】



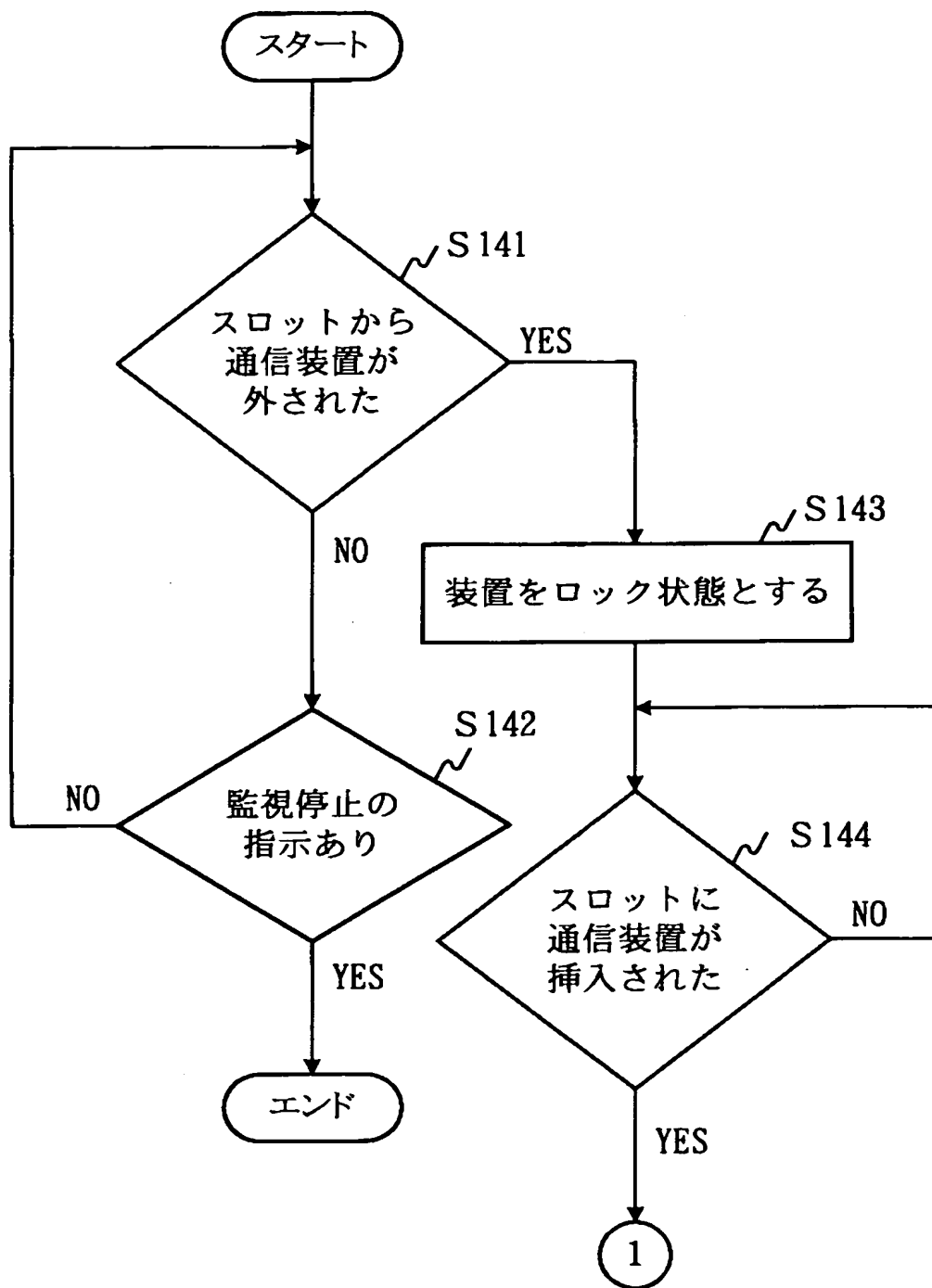
【図 2 5】



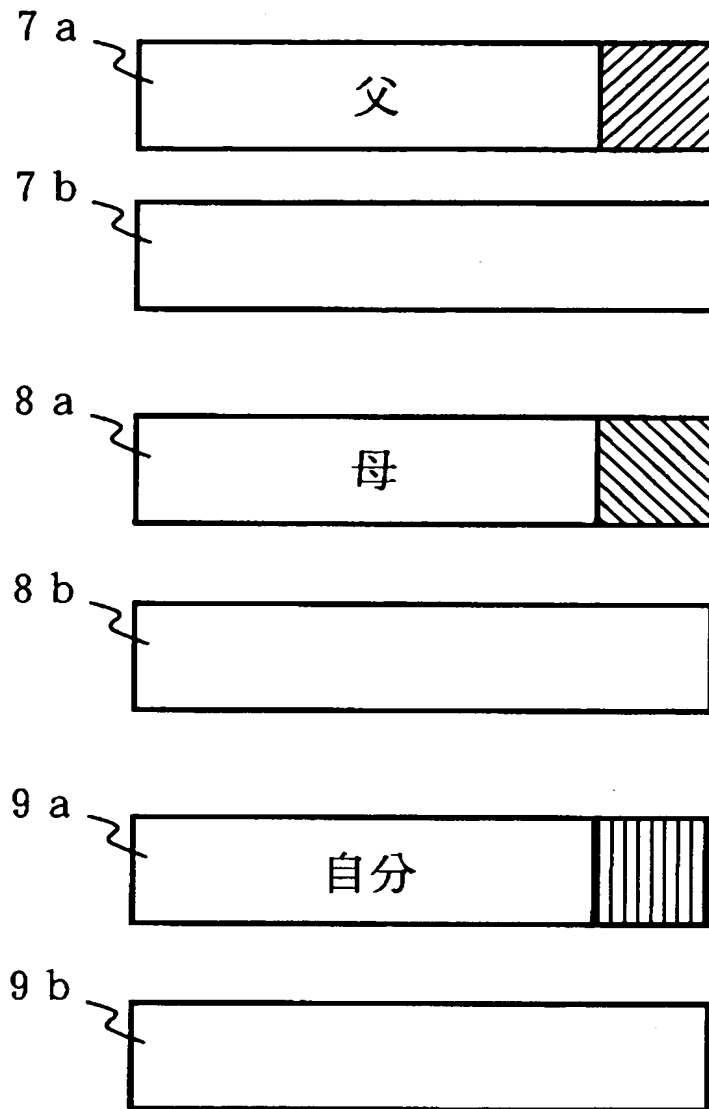
【図 2 6】



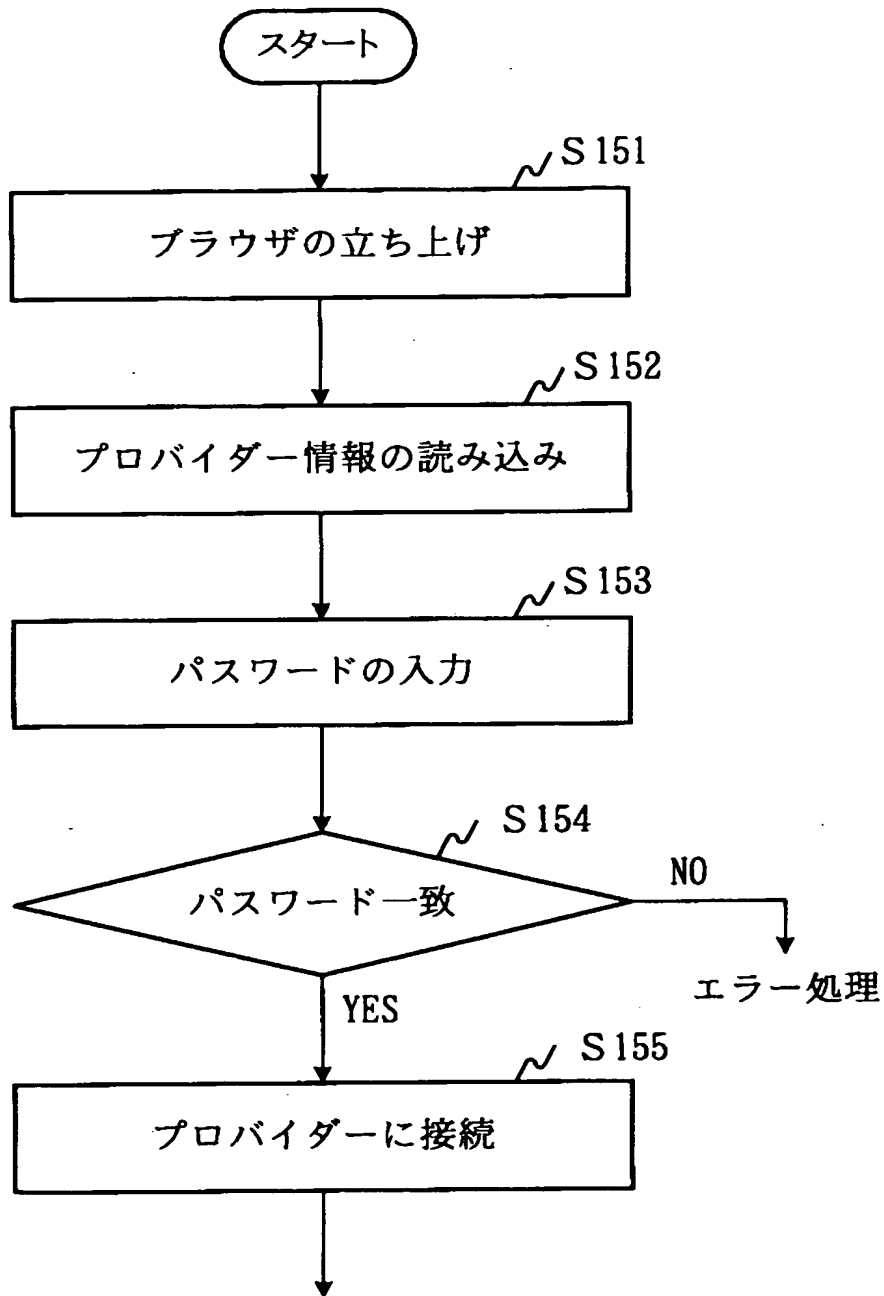
【図 2 7】



【図 2 8】



【図 2 9】



【書類名】 要約書

【要約】

【課題】 端末装置どうしを手軽にワイヤレス接続できるようにする。

【解決手段】 通信装置3a～3cのセットは規格化された形状を有する。端末1a～1cをワイヤレス接続する場合、通信装置3b、3cを端末1aのスロット2aに挿入し、通信装置3b、3cに記憶された通信アドレス及びセット固有の共通鍵を端末1aに登録する。同様に端末1bに通信装置3a、3cの、端末1cに通信装置3a、3bの、通信アドレス及びセット固有の共通鍵を登録する。その後、端末1aに通信装置3aを、端末1bに通信装置3bを、端末1cに通信装置3cをそれぞれ挿入し、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化及び復号に共通鍵を使用し、端末1a～1c間でデータを送受信する。通信装置3a～3cは端末からはみ出る部分が伝送速度に応じた色で色付けされており、色を見れば通信装置セットの種類が判別できる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日
[変更理由] 新規登録
住 所 東京都港区芝五丁目7番1号
氏 名 日本電気株式会社